ACES
OF CYBER SPADES
TOP 10 GUARDIANS OF CYBER SPACE IN 2022
REWIND <<
Comprehensive Digital Risk Protection with Cyble Vision

Capabilities

**Darkweb and Open Internet Monitoring**
- Compromised credentials
- Sensitive data leakage
- Executive brand protection monitoring
- Open-Source Intelligence

**Cybercrime Intelligence**
- Advisories on 400+ threat actors and 700+ malware operators
- Monitor 80% of Cybercrime markets
- Cybercrime conversations/mentions in forums and markets

**Attack Surface Detection & Hunting (DRPS)**
- Public facing assets
- Vulnerable assets
- Code Leakage (e.g. GitHub/bitbucket)
- Cloud buckets S3, Azure
- Malware campaigns

**Brand Reputation Monitoring (DRPS)**
- Fake/Typo Squatted Domains and Fake Content
- Fake Domains and Fake Content
- Fake app detection
- Phishing URLs
- Take downs
- Social media monitoring

**Third Party Cyber Scoring**
- Vendor risk score
- Derived from Darkweb, deep web, attack surface, public breaches, disclosures, etc

**Threat Intelligence**
- IoCs
- Security Advisories
- Compromised Cards
- BINs
- ATM PINs
Know your organization’s Darkweb Exposure

Make sure that your business continuity, compliance and operational availability is not at stake.

Scan QR code and get External Threat Profile Report customized for your organization that includes:

01 Overview of vulnerabilities in your digital risk footprint

02 Risk assessment of your attack surface and threat landscape

03 Unique Risk Score as per your darkweb exposure

04 Critical information about your leaked data and security posture

Secure your business using Cyble’s unified threat intelligence platform that offers 6 unique capabilities and 32 research parameters to deliver 360-degree intelligence.

© 2022 Cyble Inc. All Rights Reserved. contact@cyble.com | +1 678 379 3241 | www.cyble.com
Contents

7
FROM THE EDITOR
Past and Future in the same frame

10
DIGEST
The Changing Nature of The CISO in 2023

16
INSIDER
How CISOs and Security Practitioners Can Benefit From Exposure Management
How to protect your company as the digital transformation accelerates

The Arduous Task of Complying with Compliance

Cybersecurity Forecast for 2023

Aces of Cyber Spades
TOP 10 GUARDIANS OF CYBER SPACE IN 2022
Confucius once said, “Study the past if you would define the future”

The concept of cybersecurity often refers to an ongoing battle between criminals and hackers. This field is often depicted in movies and TV shows as a glamorous business. Unfortunately, the reality is the stark contrast, threats can come from anywhere, from the employee sitting next to you to foreign states and to sophisticated criminal masterminds.

Even though there weren’t any massive cybersecurity incidents like the Colonial Pipeline or Solar Winds attack of 2021, the global attacks during the third quarter of 2022 increased by 28 percent. Most of the time, attackers were focused on the educational and healthcare sectors. This gives us the opportunity to reanalyze the most critical sectors that require our immediate attention.

The year 2022 also saw a significant evolution in how threat actors operate. Instead of staying in the shadows, they disrupted the global supply chain and key industries through innovation and advanced techniques. Unfortunately, 2022 also became another year of cyber-attacks.

This issue is mostly divided into two major parts. The Year Ender section focuses on what majorly happened, while the Forecast section talks more about what can happen in 2023. More than 30 cybersecurity influencers have shared their thought on that very subject. We believe these predictions will help you make wise business decisions in the future.

This time we have also gone ahead and done our best to recognize the stalwarts of the cybersecurity industry. The Cyber Express team is proud to acknowledge the efforts of all the individuals who have dedicated their lives to protect our organizations from cyber threats.

But it was indeed a daunting task.

Due to the large number of highly skilled individuals working in the cybersecurity industry, ensuring they do their best to secure the cyberspace, it was really difficult for us to choose the best ten individuals.

But we went ahead, nonetheless, and have pulled our Aces of Cyber Spades with the Top 10 Guardians of Cyber Space in 2022. These individuals are setting a standard for excellence in the field of cybersecurity. We are also proud to announce that cybersecurity leader Chuck Brooks, is The Cyber Express Cybersecurity Person of the Year 2022.

We wholeheartedly congratulate everyone who is featured in this list. The information security sector is profoundly indebted to each one of you.

Let us know, what you liked the best in this issue. Reach out to us with your valuable feedback at editorial@thecyberexpress.com.

We wish you a Happy New Year.
With secure infrastructure...

Co-securing critical infrastructure for resilience

Cyber attacks on critical infrastructure disrupt the systems society depends on most. Choose a partner with the right expertise, right technology and right co-security approach to achieve the outcome of enhanced resilience.

For proven cyber security outcomes withsecure.com
or without?

WITH™ secure
The Changing Nature of The CISO in 2023

- By Alain Sanchez
  EMEA Field CISO

- By Daniel Kwong
  SEAHK Field CIS at Fortinet
The biggest shifts for CISOs in terms of their role in a business in the last 3 years

In recent years, the role of the CISO has shifted dramatically. With the rise of cyber attacks, CISOs are now expected not only to protect data, but also to be proactive in identifying and preventing potential threats.

In addition, CISOs are now often tasked with developing and implementing security strategies for the entire organization, not just the IT department. With the ever-changing cybersecurity landscape, CISOs must continuously adapt their strategies to stay ahead of the curve.

A decade ago, those who are now referred to as “CISOs” were not considered nearly as important as they are today. Quite often, at the time, they got answers such as, “Can’t you see I’m working?” or, “Oh no, not you again!” Today, the same people get a dedicated seat in that same boardroom. And, many CEOs ask them important questions, valuing their response. These questions actually call for answers, and perhaps the most amazing change is in the tone that is now used. “Can you provide insight into whether or not we can buy this company?” or “If you wouldn’t mind, can you prepare metrics regarding our cyber posture to present to our stakeholders next week”?

The newly regarded CISO gets a budget, a team, and the right to recruit directly. Sometimes even the voice of the CISO prevails over other long-standing professionals established on the upper floor. In fact, over the last few years, the teleworking policy, the collaborative database, legal reporting, and even the development roadmaps of innovative core applications have been placed under their direct leadership.

As we head into 2023, the role of the Chief Information Security Officer (CISO) is shifting more than ever. As cybersecurity remains a board-level discussion, and cybersecurity risk continues to increase, CISOs have substantial access within an organization, but also face significant pressure.
The transition from operations to strategic

In recent years, there has been a shift in the role of the CISO from an operations focus to a strategic one. This is due to the increase in demands placed on CISOs to protect organizations from cyber threats. In order to be successful, CISOs must now have a deep understanding of the business, its risks, and its goals. They must also be able to build and maintain relationships with key stakeholders.

One example is that the board wants more than just a service-level agreement on security incident response. Instead, they are looking for a protection-level agreement to ensure digital assets are continuously patched and protected to react to cyber incidents that may cause business disruption proactively.

Gradually, the CISO has become more involved in the decision-making processes. Almost systematically now, when innovation is involved, the CISO’s voice makes a difference. And that difference is not about saying no all the time. Rather than speaking from the voice of “Mister No” the CISO has turned into a source of inspiration for innovation, rallying data analysts and software developers under the same banner of secure operations development. To do so, the CISO and their team have initiated a healthy dialog between production, marketing, finance, and even HR and Legal. As a consequence, this has shifted the focus from bits and bytes language towards more business-oriented notions such as risk, market footprint, and compliance.

Important strategies for CISOs in 2023

CISOs should always keep in mind the importance of strategy when demonstrating business value. This means considering both the short- and long-term effects of decisions, and making choices that will benefit the company as a whole.

In the short term, it may be tempting to cut corners or take shortcuts, but doing so could jeopardize the company’s security in the long run. It’s crucial to remember that the goal is to protect the organization’s data and assets, not just to save money.
An effective way to demonstrate business value is to understand the “kill chain” of a business. Most CISOs are very familiar with the technical concept of the cyber kill chain in cybersecurity, but it’s important also to understand the impact a cyber attack can have on critical operations and the revenue or reputation loss that may result from it.

CISOs should keep the assets or data being protected top of mind, ensuring they are prioritized according to the business value kill chain. Place a higher focus on risk management tools for assets and data that have a critical impact on business operations.

The CISO should keep in mind a holistic approach when considering the benefits of the solutions. When discussing secure access, for instance, the deployment of authentication technologies could seem like a change of behavior in the eyes of users who are only exposed to VPN once a day. However, the overall benefit of a whole infrastructure dynamically protected by a holistic ZTNA strategy is far superior to securing the session, the application, or the segment. The CISO must be fluent in articulating these benefits and expressing them in terms of risks so that the stakeholders understand that the pros outweigh the cons.

**New roles “expected” of CISOs in today’s organizations**

The role of the CISO has evolved and expanded to meet the ever-changing needs of organizations. Today, CISOs are expected not only to be technically savvy but also strategic thinkers who can help organizations navigate the complex cybersecurity landscape.

In addition to traditional CISO responsibilities, such as developing and implementing security policies and procedures, CISOs are also expected to have a deep understanding of business operations and objectives. They need to be able to align their security strategies with the goals of the organization and create programs that effectively protect against cyber threats.

As the cybersecurity landscape continues to evolve, so too will the role of the CISO. Organizations will continue to expect CISOs to be innovative and adaptable leaders who can help them stay one step ahead of the latest cyber threats.
In today’s organizations, it is important for CISOs to serve as a leader of change rather than a manager of technologies. Digital transformation is such a big wave that the successful deployment of advanced cybersecurity solutions involves the entire company, all employees included. The human dimension of the role is a key success factor when you consider that 60% of transformation projects continue to fail for having underestimated the user adoption aspect. Policies that change the way people work, such as teleworking, ZTNA, or DevOps need to be explained before they are enforced. Explaining the why of cybersecurity becomes just as important as implementing the how.

**Conclusion**

The CISO’s role is no longer just about protecting the organization from cyber threats. CISOs are now a key business enabler, tasked with delivering business value.

Acting as a Risk Controller reduces operational risk and enhances the organization’s security posture by acting as a change agent. Further, today’s CISO acts as an effective communicator to the board of management to help close the organization’s cybersecurity gaps.

With more risk, more visibility, and more leadership, the role of the CISO becomes much more interesting, embracing every key department of the company, including the lines of production.

Today’s CISO is not only an expert in technologies but is also a strategist, an influencer, and a source of inspiration throughout the entire value chain.
HOW CISOS AND SECURITY PRACTITIONERS CAN BENEFIT FROM EXPOSURE MANAGEMENT
- By Kartik Shahani

Country Manager, Tenable India
The process of overhauling legacy systems and introducing new technologies undoubtedly expands the attack surface and creates more real estate for cyber attacks. Security teams within organizations don’t only have to prevent and mitigate cyber risk but also deal with the ramifications should they get breached.

A Nasdaq report suggests that after a breach becomes public, organizations accrue more than 50% of post-breach damages as long-tail costs. More alarming is the fact that 31% of expenses are incurred in the second year, and an additional 24% is incurred more than two years after the breach in highly regulated industries.

Despite the debilitating impact, organizations continue to become victims of cyberattacks. Which begs the question: Are we doing enough to manage the cyber risk in our hyperconnected world, or are we missing something?

Let’s take a look at existing realities: despite cybersecurity budgets increasing steadily over the past couple of years, fewer than 40% of CISOs say they have fully mitigated cyber risk. This is because achieving a reasonable risk posture requires CISOs and security practitioners 130 tools to detect and contain threats. That’s a lot of tools generating piles of siloed data on innumerable spreadsheets that are impossible to decipher.

To put it simply, CISOs are riddled with roadblocks, not only with the expanding attack surface but with the sheer number of security tools required to achieve a defensible posture. Does this massive problem have a solution? Yes, it does, and the answer is qualifiable exposure management.

The future needs an automated, proactive approach to cyber risk management. CISOs and BISOs must understand their threat landscape, including vulnerabilities, misconfigurations in the cloud, visibility into internet facing-asset, web apps and attack path analysis. They also need insights into how well they compare against the market and their peers in these areas. What’s more, beyond what the risk is, businesses need to learn how to mitigate and manage cyber exposure.

With a unified exposure management program, CISOs and security practitioners can help meet the demand to identify, protect, detect, remediate, respond and recover proactively. Here’s how exposure management can benefit security practitioners, managers and CISOs.
Security practitioners

One of the things that keeps security practitioners up at night is the lack of visibility into the attack surface and a unified view of all assets. An exposure management platform offers this and enables security practitioners to prioritize their efforts in remediating vulnerabilities, configurations, and entitlements. Such comprehensive visibility and prioritization capabilities help them better comprehend their attack surface, eliminate blind spots and build a baseline for effective risk management.

Security managers

When tens of thousands of vulnerabilities exist, security managers prioritize the most pressing concerns. This can be achieved through insight and context about threats, assets and privileges. It eliminates windows of risk and reduces resources allocated to remediate and respond.

For example, say the organization has 100 laptops with a vulnerability on each one of them. When viewed from siloed tools, it’s reasonable that security practitioners assume all of them are equally bad that need to be fixed immediately.

But the more important question is: How would they know whether the organization is really at risk and which laptop to fix first since there are 100 of them?

Siloed tools do not show you context. An exposure management platform, on the other hand, gives you context into the attack surface. Of the 100 laptops, it can provide context about whether the vulnerability is on the laptop of a Salesforce admin, who isn’t using multi-factor authentication (MFA) and also among them is the laptop of a front-desk clerk who doesn’t have privileged access to critical business data. This context helps security managers prioritize their efforts.

Exposure management helps security managers understand the consequences of an attack by providing visibility into how assets and users are interrelated across the attack surface. It sheds light on KPIs, giving insights into the organization’s progress over time as well as benchmark comparisons within the organization.
CISOs, BISOs and other security executives

Exposure management enables CISOs, BISOs and top executives to assess risk accurately, improve investment decisions, make decisions about insurability, meet regulatory and compliance requirements and drive improvement.

When large data sets are correlated and analyzed on one platform, it provides actionable metrics to measure, compare, and communicate cyber risk to IT and security teams and to non-technical executives and operating teams.

A single source of truth of cyber risk with clear KPIs helps measure the progress of cybersecurity programs over time and draw comparisons against industry peers.

One of the most difficult questions CISOs are often asked but find it hard to answer is: “How secure are we?” And CISOs certainly cannot answer this million dollar question by viewing the attack surface in a vacuum.

Context is critical. They need the ability to see the entire attack surface — software vulnerabilities, misconfigurations, who is using what systems and what level of access they have, whether it’s happening on a laptop, a container or an application.

Exposure management gives CISOs and security teams concise and meaningful output, painting a big picture of the attack surface along with the power of analytics. An exposure management platform answers the most important questions — How secure are we? And have we reduced our cyber exposure effectively?

The future lies in the power of data

As cybersecurity budgets increase, organizations will want to know whether their investments are paying off. CISOs and business leaders cannot rely on disparate data to make important decisions. Shoring up cyber defenses is not about outrunning cybercriminals but making it more difficult and far more costly for them to launch attacks. To achieve this level of security, organizations need to comprehend the breadth of their attack surface fully. This cannot be achieved without harnessing the power of data and a unified exposure management platform that breaks silos and works out of the box.
HOW TO PROTECT YOUR COMPANY AS THE DIGITAL TRANSFORMATION ACCELERATES
In one sense, the term “digital transformation” is outdated. Just take a moment to consider all the ways our daily lives have migrated online and how normal this has become – from video calls with friends and family to the ubiquity of cloud-based productivity tools. But in another sense, it’s still true to say that we are in the middle of a rapid and wide-ranging digital transformation. Millions of people are still working remotely, the number of connected devices continues to rise, and the process of getting accustomed to these technologies is never-ending.

While this sweeping digital transformation makes it easier to connect with loved ones and get work done, it has also created innumerable vulnerabilities for cybercriminals to exploit. From the profusion of Internet of Things (IoT) devices with rudimentary (or nonexistent) security software to the reliance on interconnected digital systems that can be hacked at many different access points, cybercriminals have an ever-expanding array of attack vectors to pursue. As new technology is released, new vulnerabilities arise. As companies oversee their own digital transformations, cybersecurity awareness should be at the center of this process. Although employee error and negligence pose the most significant cyber-risks to companies, the development of an educated workforce is the best way to mitigate these risks and protect the company. This process of cyber transformation has to be ongoing and consistent because the pace of technological change shows no sign of slowing down.

An accelerating digital transformation

The typical employee uses a dizzying array of digital services and devices on a regular basis. According to a recent Deloitte survey, the average American household has 22 connected devices, and 24% say they are “overwhelmed by the devices and subscriptions they need to manage.” Meanwhile, 54% are concerned about the security vulnerabilities created by their smartphones, and 52% say the same about smart home devices.

These concerns will likely only rise in the coming years. McKinsey estimates that the IoT market could create between $5.5 trillion and $12.6 trillion in value by 2030, which means there will be a huge influx of connected devices in the world. The cybersecurity implications of this influx are clear: hackers will have an unprecedented number of entry points, the digital line between work and home will continue to blur, and cyber awareness will be more important than ever. Companies will need to figure out how to facilitate productivity while protecting their networks from intrusion across a much wider range of attack vectors.

Continuous digital transformation is unavoidable – it’s the only way companies can remain competitive as e-commerce continues to grow, employees demand greater flexibility in how and where they work, and the number of apps and devices surges. But companies have to manage these shifts safely, which is why cyber transformation should be a top priority.

Navigating a new cyberthreat landscape

There are many ways the ongoing digital transformation puts companies at greater risk. When employees use a larger number of cloud-based communication and collaboration platforms (or rely on those platforms more heavily), they often share sensitive information in more places. The use of these platforms can also put account credentials at greater risk and provide access to other networks and systems. These dangers exist even with security mechanisms such as multi-factor authentication (MFA) in place.

For example, hackers who recently infiltrated Uber and Rockstar Games used company Slack channels to steal sensitive materials and gain deeper access to internal systems. According to Uber, using a social engineering tactic known as “MFA fatigue,” the attacker sent multiple login requests to a contractor until one was eventually accepted. This offers several lessons for companies: first, hackers have many effective strategies for circumventing security measures like multi-factor authentication. Second, third-parties can create serious cybersecurity risks for their partners. And third, widely used productivity tools like Slack and G-Suite are frequently implicated in cyberattacks.

What’s even more disconcerting is the fact that many apps and devices are less secure than the tools cited above, which are regularly updated with new security software. Smart TVs, thermostats, appliances, and other IoT devices present a target-rich environment for hackers, and they can use these entry points to infect wider networks. This is one of the many reasons home and office life has become increasingly interconnected for the purposes of cybersecurity.
Keeping your entire digital ecosystem safe

At a time when cybercriminals have never had more ways to break into your company and steal your data (or hold it hostage), it’s vital to implement a comprehensive and adaptable cybersecurity solution that can cover many attack vectors simultaneously.

With the endless proliferation of devices and cloud services out there, it’s impossible to keep track of every aspect of your employees’ ever-evolving digital lives. This is why companies have to rely on employees themselves to avoid dangerous behaviors and report potential threats as they arise.

For example, cyber-aware employees would never accept MFA requests they didn’t generate – no matter how many of those requests pop up on their phones. Instead, they would recognize that repeated requests are suspicious and report them immediately. These employees would also be careful about what they share on internal platforms like Slack, and they would beware of unnecessary IoT devices that could give hackers access to their home networks (and put their work devices at risk by connecting to those networks). Cyber-aware employees limit their exposure to cyber threats by always keeping their devices updated, sharing sensitive information on a need-to-know basis, and avoiding dubious third-party apps.

The cyber transformation requires companies to provide these lessons with engaging, digestible, and relevant content that employees will embrace. As cybercriminals continue to identify and exploit new attack vectors, companies can only hope to fill these security gaps with educated employees who are aware of those vulnerabilities as well. This is how your cyber transformation will stay one step ahead of your digital transformation.
Privacy is a right that keeps people feeling safe while a violation of it in the face of data hacks causes not just financial loss to the company but also mental trauma to its victims.
The Arduous Task of Complying with Compliance

To maintain data security, following compliance guidelines is a must to avoid falling under the judgment of regulatory bodies. Organizations and companies, whether small or large, are expected to follow compliance standards set forth to safeguard the privacy and data of the individuals it belongs to.

Cybersecurity compliance makes it mandatory for users to follow regulatory requirements that apply to them. Regulations and standards created by experts working in agencies, law, and other authorities are followed by establishing risk-based controls that safeguard data confidentiality, integrity, and availability (CIA). Governmental bodies, along with legal agents, have put forth offices that keep a keen eye on data irregularities that take action when required. The Health Insurance Portability and Accountability (HIPPA) Act, the New York Department of Financial Services (NYDFS), and the General Data Protection Regulation (GDPR) are some of them. The Family Educational Rights and Privacy Act (FERPA), the California Consumer Privacy Act (CCPA), the Children’s Online Privacy Protection Act (COPPA), and the Cybersecurity Maturity Model Certification (CMMC) are among others. The Personal Data Protection Law (PDPL) is the law for the Kingdom of Saudi Arabia. Each body regulates data handling violations in its respective sector.
1. **HIPPA** – The Health Insurance Portability and Accountability (HIPPA) Act or the Kennedy-Kassebaum Act maintains that the personal health information (PHI) of individuals seeking medical attention, in any capacity, is not violated. It applies not just to healthcare providers in the United States of America but also to clearing houses, healthcare plan providers, and other service providers handling data.

2. **NYDFS** – The New York Department of Financial Services applies to covered institutions that require the department of financial services (DFS) licensure, registration, or charter in New York. Companies that fall under NYDFS offer facilities like mortgages, insurance, licensed lenders, and foreign and private banks. This regulation seeks to have a dedicated Chief Information Officer (CIO) hired to make sure the parameters of data security are met in the business.

3. **GDPR** – The General Data Protection Regulation applies to all EU citizens throughout Europe including Iceland, Norway, and Liechtenstein. It is applicable to European Union member states, and the European Economic Area (EEA).

   It seeks to make sure the seven principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability are met. GDPR is considered one of the stricter regulations and offers about eight rights to users. Those include the right of access, to be informed, to erasure, to restrict processing, data portability, to object, and to rectification.

4. **FERPA** – The Family Educational Rights and Privacy Act oversees the security of information of students. Educational records are to be protected by schools that receive funding from the United States of America’s Department of Education where this regulation applies. FERPA gives rights to parents also in terms of educational records, such as to inspect, review and request corrections if the records are inaccurate. Schools are allowed to charge a fee if records are asked for reference. Also, this must be done by eligible students or parents based on written permission and not randomly, which would result in a violation of privacy.

5. **CCPA** – The California Consumer Privacy Act applies to the residents of California and was enacted into law in 2018. It applies to companies working in California and makes a minimum of $25 million annually. It must either make more than half of its profit from collecting user information or processing data of over 50,000 users. The users need not be residents of California.
. Personal data includes, however, is not limited to real and alias names, postal addresses, social security numbers, IP addresses, and online identifiers. The details maintained by the government that is publicly available may not be considered personal information.

6. **CMMC** – Propagated by the United States Department of Defense, the Cybersecurity Maturity Model Certification applies to US companies that process controlled unclassified information (CUI). It does not apply to all US government contractors but only to Department of Defense contracts. Since 2020, DOD contractors need a third-party audit and certification to ensure they are meeting adequate cybersecurity controls.

7. **COPPA** – The Children’s Online Privacy Protection Act applies to businesses and website operators that must take the consent of the parents of children under the age of thirteen in terms of collecting and using their personal data. The consent should be verifiable. The COPPA compliance is applicable to companies that are outside of the United States of America if it handles the data of residents.

8. **PDPL** – The Personal Data Protection Law of the Kingdom of Saudi Arabia is its first-ever data protection law that protects data that is processed, disclosed, collected, and retained by organizations. It also looks after cross-border data transfers and will go into effect on 17 March 2023. The Saudi Data and Artificial Intelligence Authority (SDAIA), which is the regulatory authority of Saudi Arabia, and the National Data Management Office (NDMO) have also issued a draft of the executive regulations in March 2022 that outlines the various data-related details that must be heeded by.

Those within the United Arab Emirates (UAE) who are processing or controlling the data of residents of the UAE whether living in or outside of the country must comply with the PDPL. The regulations apply even to deceased persons whose data must not be violated.

### Following a cybersecurity compliance standard for companies

Different sets of compliance guidelines are set by different bodies belonging to various countries and regions. Having a chief information security officer (CISO) is required to oversee the way the enterprise handles data and how best to improve solutions for the same. IT managers, chief operating officers, chief information officers, and chief technology officers may also offer insights into this area along with a CISO.

### Maintaining compliance

In a survey conducted by IBM, it was revealed that nearly 50% of employees are unsure about accessing cybersecurity tools and threats in the work-from-home setup. Added to that, new employees are offered very little training in detecting and reporting threats and suspicious online activities. The staff can get confused, threatened, and may panic in order to preserve their job.

Moreover, password management know-how can be poor among employees that may or may not be working in technologically advanced setups, which can make it easier for hackers to breach into their systems. Seeing that one’s company is following compliance guidelines requires being diligent about a couple of things. Compliance requires making sure that the following areas of work are taken care of -

1. **Identifying the type of data held within the systems**
2. **Having a CISO investigate data processing within the company**
3. **Maintaining regular risk and vulnerability assessments**
4. **Making sure the technical controls are in place in keeping with tolerance and requirements**
5. **Implementing all the required policies, procedures, and process controls**
6. **Keep reviewing and testing the solutions to make sure it meets the requirements**
Running a business requires not just keeping a tab on finances, products, and plans. Today, data privacy has become one of the most crucial entities to preserve while handling it as part of business solutions. Restrictions are placed on who can share, access, and keep data and for how long in the ever-evolving policies.

Violations coming from unauthorized access can lead to publishing the data on cybercrime forums, selling it for impersonation and debiting money from spoofed cards, seeking false insurance claims with forged documents, and launching socially engineered attacks to whomsoever can be manipulated using their own data.

Users may get bombarded with spammy and fraudulent communications, while investigators start looking for mishandling of data in several systems and networks. Legal bodies investigate minute details of where, how, when, and with whom the data was shared. And the company risks losing its reputation, market value, and loyalty of its customers.

In the recent Medibank data leak, details of patients the company held were dumped on the dark web by hackers. Australia suffered greatly in 2022 with reference to data breaches and data leaks, which led to the drafting of stricter bills and amending them. Abortion details, medical transcripts, names, etc. were posted for anyone to see with access to the dark web. This raises questions on the basic right to privacy of individuals.

Hence, compliance plays a crucial role to make sure every individual associated with business, enterprise, and organization is considerate and well aware of how data is being handled.

**Data breach**

Data is the fuel of all companies regardless of sector. Mishandling of data can lead to complications involving compliance. Breached data can fall under the broader areas of personally identifiable information (PII), financial information, and protected health information. Other details about users’ race, religion, and biometric data also need to be protected to not default on data handling laws of the region.

Companies need to secure their emails and IP addresses from breaches and unauthorized access because it can give away a lot about whom it belongs to, leaving them vulnerable to attacks.

**Among personally identifiable information, these details must not reach hackers:**

1. Date of birth
2. Full or part of the name
3. Address
4. Social security number (SSN)

**Financial data that must be secured by enterprises and businesses are as follow:**

1. Credit and debit card numbers, expiration and card verification values (CVV), personal identification numbers (PINs), and credit history and ratings.
2. Bank account details

**Protected health information that organizations and the healthcare sector must secure:**

1. Patient prescription details, and medical history
2. Hospital admission records, and appointment history
3. Insurance records
Data compliance is a framework that everyone falling under it must follow, failing to do so can bring about monetary fines and other legal penalties, such as class action lawsuits. Class actions like securities litigation and civil rights class action involve relief settlement. Class action lawsuit, also called group claim lawsuit, mentions the individual who was impacted by the data incident, what they expect in compensation if they do, the details of the incident, and so on. 

Who can file a class action lawsuit?

Any individual and any number of individuals can file a class-action lawsuit with interest in the incident.

According to Rule 23(c)(3), it may need to be filed in a relatively timely manner and besides the details of the claim issue, it needs information about the defenses and the effect of a class judgment on the members.

The more the number of people impacted or filing the complaint, the better its chances of being taken in as a claim. The sum decided for settlement may also be as high or low as deemed appropriate by the court.

The largest amount paid for a data breach

The largest ever non-compliance fine for data-related incidents was paid by Equifax with an amount of $700 million. Equifax, which offers several services such as credit monitoring and identity theft protection, was held for a data breach of over 147 million Americans in 2017, for which it had to pay the sum as the lawsuit demanded.

To keep lawsuits away, not lose credibility, and follow the compliance guidelines, it is essential to keep not just a CISO to ensure compliance but also to train the staff in data and security. Every employee that handles data must feel confident to report an incident or suspicious activities to the concerned department. Failing to follow the standard course of action can lead to a graver impact.
YEAR ENDER
Securing The Cyber Space:

Top 10 Cybersecurity Startups in 2022

Security-based firms are growing rapidly, and there is a good reason why they are doing exceptionally well in terms of protection and profitability. For starters, cybersecurity professionals have the knowledge and experience to detect, prevent, and respond to cyber-attacks.

While cyberattacks have increased in numbers, the defenders have also boosted the corporate infrastructure, and its estimated value in 2022 is around USD 173.5 billion. It is projected to grow to USD 266.2 billion by 2027. The Compound Annual Growth Rate (CAGR) of 8.9% from 2022 to 2027 goes to show that cybersecurity is a promising domain for making a sustainable internet experience.

In this stratum, big corporations and SMEs are growing at the highest CAGR during the forecasted period. To secure systems from attacks, cybersecurity startups are employing new tools and strategies that may be unknown to traditional companies.

Cybersecurity firms also use advanced analytics to discover patterns of harmful activity and respond rapidly to secure the system. They also employ powerful encryption and authentication mechanisms to keep data secure.

The entire catalog of cybersecurity and everything it offers is an immediate requirement for the modern world and is vital in protecting our data, networks, and systems. Cybersecurity is an ever-evolving field, and it is essential to stay up to date on the latest developments and trends.

The Mandiant acquisition, where Google closed the $5.4 billion deal with the security company in September 2022, is one of the few examples of how cybersecurity has become mandatory in the world of economics and business. Google has also increased its area of interest in security programs, and with the addition of Mandiant, SMEs and corporate organizations look forward to better mitigation opportunities.
Protecting oneself and the data from cyber threats becomes easier when one understands cybersecurity fundamentals. Many cybersecurity start-ups are working towards making the world more secure. In this article, The Cyber Express bring you the top 10 cybersecurity start-ups in 2023 that aim to enhance security and take it to the next phase of evolution.
Fireblocks

Established in 2018, Fireblocks is an end-to-end encrypted cloud service provider. With Fireblocks, businesses can employ better security over their digital assets. It also helps them in secured trades, exchanges, and commerce, protecting data at every step of the commercial chain.

Since 2018, the company has raised over $1B in funding over five rounds and is backed by 29 investors, including Spark Capital and ParaFi Capital. Fireblocks has provided its services in the banking, fintech, OTCs, and hedge funds industries and offers security and control for its clients.

Fireblock boasts a wide range of products and services specially curated for businesses at all levels and revenue. The company acquired two organizations — First Group in five funding rounds between 2019 and 2021.

Snyk

Snyk is the first code vulnerability scanner for npm, RubyGems, and Maven and provides a platform of databases covering one million unique vulnerabilities. The company offers security aid to businesses and has over an ROI of $2.1 million by reducing risk throughout the SDLC.

Snyk has funding of $1B from 34 investors, including Sands Capital Ventures and Evolution Equity Partners, and has acquired seven organizations within eight years since their inception. The newest acquisition of TopCoat Data happened on March 7, 2022, making Snyk one of the best choices for businesses opting for security suits.

The company claims itself as the first developer-first company and boasts its security-intended products as the USP. These security products help mitigate and save time and money, enhance productivity, higher revenue rates, and better customer satisfaction. According to the company's report, about 1,200 businesses use Snyk, including Google, Intuit, MongoDB, Salesforce, and more.
Aura

In the first four rounds of funding, the American-based cybersecurity firm Aura raised $500.7 million and has been working towards providing a unified digital threat protection platform that offers security products and services for businesses around the world. Six investors have backed the company, wherein the Madrone Capital Partners, Accel, and Circle Media are the recent ones. Aura is predicted to be among the most financially secure startups in 2023.

The company is dedicated to creating a safer internet experience for its clients. With their state-of-the-art tools and mitigation techniques, big corporations like Money, TechRadar Pro, and Forbes are one of their clients. Moreover, the company’s innovation and security tools help create a safer world by continuously evaluating threat actors’ campaigns and hackers who exploit vulnerabilities in the open.

Semperis

Founded in 2014 and headquartered in Hoboken, New Jersey, Semperis is one of the biggest startups of this decade that gained financial success in its journey. With a specific set of tools and personalized service plans, Semperis is one of the most sophisticated cybersecurity providers in the space.

The company offers identity protection and cyber resilience for cross-cloud and hybrid environments. Its continuous efforts raised $240 million in funding from 7 rounds and boarded 17 investors, with Insight Partners and Paladin Capital Group being the most recent investors.

Semperis’ last round of funding was on May 24, 2022, with Series C. The company’s flagship product offers identity protection for companies and businesses, helping them recover from losses quickly and continuously evaluating risk management and mitigation against cyberattacks. With that, the company has created a strong funnel for clients, where Fortune 500 companies and enterprises all over the world are regular customers.
Cyble

Known as the world’s fastest-growing threat intelligence provider (YC W21), Cyble is a team of influential researchers and engineers who aid customers in their cyber risk management using AI-powered actionable threat intelligence. The company was founded in 2019 by Beenu Arora and Manish Chachada and is known for being at the forefront of hacking, and dark web filtering.

Cyble is known for its security-rich flagship products. Cyble Vision, AmIBreached, and Cyble Hawk offer deep insights into cybercrime, giving an eagle-eye view to gathering intelligence across the Deep Web, Dark Web, and Surface Web to provide actionable threat intelligence.

Since its inception, the company has raised $14.6M in funding over 9 rounds with 11 investors and is backed by famous capital investment firms like January Capital and Spider Capital. The company’s latest round of funding was held on February 22, 2022, from a Series A round.

Orca Security

Founded by Avi and Gil Geron in 2019, Orca Security offers patented SideScanning technology and Unified Data Model to help companies protect their data against cyber threats.

The organization uses sophisticated AWS, Microsoft Azure, and Google Cloud Platform technologies to provide insights into a company’s cybersecurity posture and how companies can prevent damage to their digital assets.

The security organization has raised a total of $632M in funding over 5 rounds of investment and has 17 big prolific investors on board, such as ICONIQ Capital and Splunk Ventures. Orca Security acquired one organization, RapidSec, on January 19, 2022.

Orca provides aid to its clients using its trailblazing list of cloud detection features and prevents companies from hackers, scammers, and malware attacks. It works with Google Cloud Platform, Microsoft Azure, and Amazon Web Services to provide a better security environment for companies to grow to their highest potential.
SecurityScorecard

SecurityScorecard is one of the fastest-growing security organizations that help businesses and corporations predict and remediate risks. The company has raised $292.2 million in its 8 rounds of funding with the latest E Series round.

With 19 investors, including the latest investment from Kayne Anderson Rudnick and Accomplice, SecurityScorecard offers a sophisticated platform for dealing with cyber threats and protecting firms by providing them with cybersecurity posture reports. According to PrivCo, SecurityScorecard’s post-money valuation ranges from $1B to $10B.

As for its acquisition status, the company acquired LIFARS on February 7, 2022, and has over a million companies continuously rated for their cybersecurity posture, providing peace of mind to their clients.

The company’s core features include self-monitoring tools, cyber insurance, third-party risk management, and others. Over 1000 organizations use SecurityScorecard’s patented rating technology for cyber self-monitoring, third-party risk management, board reporting, and cyber insurance underwriting.

ZeroFOX

Founded in 2013, ZeroFOX has a stronghold in the cybersecurity sector and is one of the leading firms that provide security services, including aiding companies with external threat intelligence, protection, and response solutions that provides organizations with comprehensive visibility and protection across the surface, deep and dark web.

In its five rounds of funding since 2013, the company has raised a total of $154.2M in funding from Series Seed Round to Series D, with the latest investment from Intel Capital.

ZeroFOX has acquired two companies since their inception, Vigilante ATI and Cyveillance. Coming to its features, the company provides a monitoring platform for social media channels. The company has secured several awards, including the SINET16 Champion, Security Tech Trailblazer of the Year, and one of CRN’s Top 10 Security Companies.
CyCognito

CyCognito is a completely automated and highly scalable external cyber risk management company that assists companies by eliminating threats and building resistance against hackers. The company uses sophisticated tools and programs that work silently in the background and do not disrupt normal functioning and operations.

Coming to its features and what it offers, the company provides a platform for external cyber risk management designed to go beyond traditional attack surface management. It is fully automated, extremely scalable, and built to perform as promised.

CyCognito has raised $153 million in four rounds of investment, and their most recent funding came in the form of a Series C round on December 1, 2021. CyCognito has 13 investors, with Thomvest Ventures and Harpoon being the latest addition to the list.

CyberGRX

CyberGRX offers a global cyber risk exchange as part of its third-party cyber risk management program. CyberGRX has received $99 million in investment over six rounds. Their most recent fundraising came from a Series D round on December 10, 2019. The security provider has 14 investors, including the latest ones, such as Scale Venture Partners and AllegisCyber.

The company has a post-money valuation of $100M to $500M as of December 10, 2019 and has been scaling its clientele by providing better support in cyber risk management. CyberGRX offers a sophisticated platform for identifying, assessing, mitigating, and monitoring an enterprise’s risk exposure across its entire partner ecosystem at a low cost.

Its system, through automation and advanced analytics, enables organizations to collaboratively minimize vulnerabilities posed by their increasing reliance on vendors, partners, and consumers.
Game of Thorns:

The fall of the high and the mighty after the backstabbing of an ally; A crucial decision resulting in changing allegiances; Conspiracy, treachery, and backlashes; New warlords rising after the fall of the sovereign; The murky world of ransomware in 2022 had all the elements of a full-blown Game of Thrones-style costume drama.

Security firms across the world detected more than 2,000 ransomware attacks of different scales using about 30 popular variants of encryptors. Ransomware gangs targeted the US region the most, and the most attacked sector was industrial goods and services.

In addition, there has been an increase in politically motivated data extortion attacks, some of which are believed to be coordinated by state-sponsored actors. However, what added excitement to all these affairs was the spectacular fall of the mighty Conti ransomware gang, LockBit’s ascension to the top slot, and eventual displacement by others.
Conti falls, LockBit rises

LockBit emerged as the ransomware market leader after the shutdown of the Conti gang following the famous ‘ContiLeaks’.

After Russia invaded Ukraine on February 24, 2022, the Conti operators publicly expressed their support for Russia. However, a few days later, an anonymous Twitter account called “Contileaks” released a collection of internal chat messages from Conti dating back to 2021. The account also published additional internal chats from 2020.

As a result, Conti’s operators began to dismantle their operations. In May 2022, the main Conti platform was shut down and split into several smaller units, which allowed the group to be more agile and evade law enforcement. About a month later, the Conti’s Ransomware-as-a-Service (RaaS) operation ceased its data leaks and negotiation activities.

Conti affiliates, or individuals or groups who perform intrusions and ransomware distribution for a share of ransom payments, joined other players in the ransomware-as-a-service (RaaS) market, with LockBit being the primary beneficiary.

Although LockBit has been active for a similar length of time as Conti, it has been overshadowed by other groups like Maze and Ryuk in its first two years of operation. However, the release of version 3.0 of its ransomware and affiliate programs in June helped it become the leading ransomware strain in the third quarter.

However, the situation changed in September when the internal details about the LockBit affiliate program, builder for the ransomware, and supposed leader were leaked, damaging the group’s reputation. This led to a comparative decrease in LockBit breaches in the third and fourth quarters of 2022.

From the ashes of Conti

Gangs like Black Basta, Hive, ALPHV/BlackCat, and Stormous soon caught up. However, researchers pointed out many similarities between Conti’s operation and that of Black Basta and Hive.

Black Basta affiliates prefer highly profitable organizations across geographies, while Hive seems to have a more restricted focus, with an alleged Hive operator disclosing in August that the group’s affiliates primarily target organizations in Australia, Canada, the UK, and the US.

According to Intel 471 researchers, actors deploying the Hive ransomware often use phishing campaigns to gain initial access and distribute their malware, and that these campaigns are usually written in English, which allows the group to refine its social engineering efforts and tailor them to a specific audience, likely reducing resource expenditure and increasing the chances of success.

The ALPHV RaaS affiliates, on the other hand, seem to prefer exploiting vulnerabilities and exploits to gain access to large organizations. The alleged leader of the ALPHV RaaS operation claimed in September that the group had targeted airports, fuel pipeline operators, gas stations, oil refineries, and other critical infrastructure since the affiliate program was launched.

Other notable ransomware variants that came up include AvosLocker, Vice Society, BianLian, Medusa, Ransomhouse, Quantum, and LV.

Clones galore

Researchers at Cyble noted a clear pattern of Conti techniques in a stream of ransomware in the Q2 and Q3 period. A new strain of ransomware, created from the leaked source of Conti called itself Putin Team in an explicit attempt to appear Russian, according to the Cyble Research and Intelligence Labs (CRIL).

The CRIL report lists the tactics of three other versions: ScareCrow, BlueSky, and Meow.

“BlueSky follows a different encryption scheme, but for rest of the ransomwares resembles to Conti ransomware,” noted a CRIL researcher.
ScareCrow encrypts the files and appends .CROW as an extension and drops a ransom note named “readme.txt”, which contains three Telegram handles to contact the threat actor. Meow ransomware follows the same path but encrypts the victim's files and append .MEOW as an extension.

However, BlueSky exhibits several traits of Conti as well as Babuk ransomware. The source code of Babuk ransomware was also leaked in 2021.

“Upon execution, the BlueSky Ransomware encrypts files and adds .BLUESKY extension to them. The ransom note dropped by this ransomware is named, "# DECRYPT FILES BLUESKY #.txt" which contains instructions for decrypting the files. This ransomware group uses an onion site to interact with the victims,” said the CRIL report.

More regions, higher scale

According to CRIL, the top countries targeted by ransomware since 2019 were the US, France, Spain, the UK, Germany, and Italy. While the top four are the usual target, Italy's entry on the list was the direct result of its support for Ukraine against the Russian invasion.

“The ever-increasing threat landscape due to the Russia-Ukraine conflict has fundamentally transformed the attack surface due to frequently disclosed vulnerabilities and exposures. Meanwhile, the increasing complexity of tools and techniques adopted by the threat actors has revealed the gaps in the cybersecurity infrastructure of Italian organizations and entities,” said a Cyble advisory about cyber-attacks on Italy.

Australia was another hotbed for ransomware action, with high profile breaches such as telecom giant Optus and insurance major Medibank.

The sectors that were most frequently targeted by ransomware attacks include industrial goods and services, industrial and consumer products, technology, construction and materials, manufacturing, professional services and consulting, travel and leisure, and public services.

Here are the ransomware cases we saw in 2022, notable for their scale, damage, and sometimes mere quirkiness:

In January, the Lockbit ransomware group claimed to have successfully hacked the French Ministry of Justice, threatening to release the organization’s data on the Dark Web if a ransom was not paid by February 10.

In February, the BlackCat ransomware group launched an attack on German oil company Oiltanking, causing disruptions at gas stations nationwide. Royal Dutch Shell reported that it had to redirect its supply depots due to the incident, and according to Handelsblatt, 233 gas stations in Germany were impacted and had to rely on manual processes. The attack had a widespread effect on the country’s fuel supply chain.

The Hive cybercriminal group in February targeted Syndicat Intercommunal d’Informatique (SII), an IT service provider based in France. SII provides IT services to several municipalities within the Department of Seine-Saint-Denis in the Île-de-France region, and at least three of these municipalities were also affected by the ransomware attack.
Global graphics card major Nvidia Corp was targeted by the Lapsus$ ransomware group in March. The company released a statement acknowledging the attack, but did not provide any further details. According to the hackers, Nvidia decided to fight back rather than negotiate, and reportedly exfiltrated 1TB of data from the group. Security researchers shared screenshots from the Lapsus$ Telegram channel on Twitter, where the gang claimed that Nvidia had launched a retaliatory strike to prevent the release of stolen data.

In March, the Lapsus$ data extortion group leaked confidential data that they claimed to have obtained from electronics giant Samsung. After the attack, the gang shared a note taunting Samsung and included a snapshot of C/C++ directives in Samsung software, indicating that they had accessed the company’s data.

French video game company Ubisoft confirmed in March that they had suffered a hack at the hands of the Lapsus$ gang. In a statement they said, “we can confirm that all our games and services are functioning normally and that at this time there is no evidence any player personal information was accessed or exposed as a by-product of this incident.”

In April, the Costa Rican Government’s computer systems were hit by a ransomware attack carried out by the Conti group. After the government refused to pay a ransom, the group began publishing stolen information.

The Costa Rican finance ministry was the first to report issues, including disruptions to tax collection, and attacks on the social security agency’s human resources system and the Labour Ministry followed. The pro-Russian Conti Group demanded a $10 million ransom in exchange for not releasing the information stolen from the Ministry of Finance, which could include sensitive data such as citizens’ tax returns and information on companies operating in Costa Rica.

Worsening the crisis the Hive Ransomware Group hit the Costa Rican Social Security Fund on May 31, 2022, forcing the institution to shut down all its critical systems, including the Unique Digital Health File and the Centralized Collection System.

The Rio de Janeiro finance department announced in April that it had suffered a ransomware attack on its systems. The LockBit gang claimed to have stolen 420 GB of data, which they threatened to release if the ransom was not paid.

Stormous ransomware group, a newbie gang, in April claimed to have hacked Coca Cola’s servers and obtained 161 gigabytes of data, including financial information, passwords, and commercial accounts. They are now attempting to sell the data for over $640,000 or more than 16 million in Bitcoin. Coca Cola is investigating the incident.

In May, India’s Spicejet airlines reported that it had experienced an “attempted ransomware attack,” leading to significant delays and leaving passengers stranded at airports with little communication from staff. The company stated that its IT team was able to contain and resolve the issue but did not provide any further details on the attack or the perpetrators.
In May, Cisco reported that the Yanluowang ransomware group had breached its corporate network and attempted to extort the company by threatening to leak the information it had obtained. Cisco believed that only non-sensitive information had been stolen, and the data was accessed through a Box folder linked to a compromised employee’s account that had been hacked through a personal Google account with synced information. Despite the breach, Cisco did not identify any impact on its business, though 3,100 files (2.75GB) of data related to the incident were later published on the dark web.

In May, state-owned airline Tap Air Portugal in Portugal was hit by a ransomware attack claimed by RagnarLocker. The airline claimed that no data was stolen, but the attack affected its website and app. However, RagnarLocker released a screenshot of the passenger’s personal information and suggested that “hundreds of Gigabytes may be compromised.” It is unclear if the group demanded a ransom from the airline.

In June, retail giant Walmart denied reports that it had been hit by the Yanluowang ransomware group, a newly discovered cybercriminal. According to Walmart, its “Information Security team is monitoring our systems 24/7” and believed the claims to be untrue. A post on a data leak site claimed that the group had breached Walmart and encrypted between 40,000 and 50,000 devices.

In September, the Holiday Inn hotel chain experienced disruptions in their booking channels and other applications due to a cyberattack. The attack was carried out by a couple from Vietnam who accessed the company’s databases with the weak password Qwerty1234. The Intercontinental Hotels Group, which owns Holiday Inn and other hotels, did not report any data loss during the “unauthorized access” to their technology systems. The hackers told the BBC that they carried out the attack “for fun.”

In the cyber attack that put Australia on the cybersecurity news, an unidentified ransomware group in September claimed to have obtained data belonging to 11.2 million users of the country’s second-largest telecommunications company Optus. The criminals demanded $1 million in Monero cryptocurrency to prevent the sale of the stolen data. The Australian federal police are currently investigating the incident.
In October, the Everest ransomware group targeted South African state-owned electricity company ESKOM, which supplies more than 90% of the energy to customers in South Africa and the SADC region. The company experienced some server issues during the attack and the ransomware group published a notice announcing the sale of the company’s root access for $125,000 and claimed to have access to all servers with root access to many. ESKOM received a ransom demand of $200,000 for the return of the stolen data and access, but it is unclear if the company plans to pay the ransom.

Medibank, a major medical insurance provider in Australia, experienced temporary outages in October due to a ransomware attack. It has since been revealed that all customer data was accessed during the incident.

In November 2022, the hacker group, allegedly associated with Russian ransomware group REvil, released Medibank customer data on a dark web blog after the company reportedly refused to pay the US$9.7m ransom. By December 1, reports indicated that the hacker group had released all remaining compromised files in their possession.

In the same month, UK car dealership company Pendragon that operates 200 dealerships across the country and oversees multiple brands was targeted by the LockBit group in a ransomware attack. The group demanded a ransom of $60 million, but Pendragon refused to pay and has since obtained a high court injunction against LockBit.

In November, the LockBit ransomware group targeted French defense and technology firm Thales with a ransomware attack. While Thales denied that its systems had been hacked, it did confirm that data had been stolen from a user account. LockBit subsequently leaked 9.5 GB of archive files, which are thought to include corporate and technical documents, and claimed that they had also stolen commercial documents, customer files, accounting files, and software from the company.

LockBit ransomware group targeted German multinational automotive group Continental that month, selling stolen files for $50 million on their leak site. Negotiations between the two parties reportedly failed, but the ransom amount requested was not disclosed.
A Costa Rica-like incident repeated in Vanuatu, a small archipelago in the South Pacific, in November. A ransomware attack caused widespread disruption in official government email addresses stopped working and websites for the island’s parliament, police, and prime minister’s offices were disabled. Intranets and online databases for schools and hospitals were also made inaccessible. No group claimed responsibility for the attack.

During the same month, Malaysian low-cost airline AirAsia fell victim to the Daixin Team ransomware group. The group claimed to have obtained personal data for five million unique passengers and all of the company’s employees. Samples of the stolen data, including passenger and employee information, were uploaded to Daixin’s leak site.

In a separate incident, the ALPHV/BlackCat ransomware group targeted Thailand-based low-cost airline Nok Air. The group claimed to have exfiltrated over 500GB of data from the company and posted some of the stolen information on their leak site.

In late November, a suspected ransomware attack impacted servers at the All India Institute of Medical Science (AIIMS). This caused delays for patients as registration, sample processing, and billing computers went offline. All services were forced to operate manually while the incident was being resolved. An investigation with law enforcement authorities is ongoing, and measures are being taken to prevent further attacks.

The Guardian newspaper faced a “serious IT incident” in late December that affected access to all its offices. Employees were advised to stay home and stay away from VPNs.

“There has been a serious incident which has affected our IT network and systems in the last 24 hours. We believe this to be a ransomware attack but are continuing to consider all possibilities,” a Guardian Media spokesperson said in an email to The Cyber Express.
The Empire Strikes Back

As the attacks on the APAC region intensified, cybersecurity threats turned truly global in 2022. It was also the year when the respective governments were up in action: some tightening their policies, some their agendas.

Cyber policy is a tricky business. Criminals have no ethics, honour, or compassion and care about nothing other than their cause and greed. Their actions are swift and the damage intensive. Policymaking stand at the other end of the spectrum, bound by civic, economic, and political considerations.

2022 was the year when cybersecurity legislations across the world decided to stop playing catch-up and get government defence up to speed, or at least try. The changes were strikingly visible in South Asia and the APAC region, which saw large-scale cyber-attacks spike in 2022.

The Indian administration used this as an opportunity to enhance government control and monitoring over the Internet, while the Singapore government shifted the onus of cybersecurity to the private sector by imposing a licensing norm.

Australia, meanwhile, focused on improving the accountability of data-managers – from organisations to individuals – by imposing the probability of a penalty that could go up to $50 million.

Curiously, they all, in some way or the other, relied on the US for the baselines of cybersecurity regulations.
It all began in the West

On June 21, 2022, two cybersecurity bills were signed into law by US president Joe Biden, as part of a series of efforts to improve the country’s cybersecurity and improving coordination on security issues at all levels of government and build skills and experience among the federal cyber workforce.

The State and Local Government Cybersecurity Act was meant to improve coordination between the Cybersecurity and Infrastructure Security Agency (CISA) and state, local, tribal, and territorial governments by allowing them to share security tools, procedures, and information more easily.

The Federal Rotational Cyber Workforce Program Act allowed government employees in IT, cybersecurity, and related fields to rotate through roles across agencies to gain new skills and experience in various job functions. According to the statements issued on these legislations, these laws come amid a trend of increased efforts to strengthen cybersecurity at the federal, state, and local levels, including the passage of the Cyber Incident Reporting Act in March, which requires organizations in critical infrastructure sectors to report a cyberattack within 72 hours and a ransomware payment within 24 hours.

What expedited these moves were the sweeping ransomware attack on Puerto Rico, which brought the US territory, Puerto Rico, to its knees.

“At least 40 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity. Twenty-four states enacted at least 41 bills in 2022 so far,” said the briefing issued by the US National Conference of State Legislatures in July.

Indian government and tighter internet control

The Indian Computer Emergency Response Team (CERT-In) in June issued new cybersecurity guidelines under the Information Technology Act, 2000 (IT Act) “in response to the significant number of cybersecurity incidents” that happened in the country.
Reported incidents, including data breaches and ransomware attacks, reached a total of 1.4 million in 2021 and 212,000 in the first two months of 2022. The new guidelines that went into effect in June 2022 apply to service providers, intermediaries, body corporates, data centers, and government bodies and require the reporting of cybersecurity incidents within six hours.

To ensure the timeliness of reporting, they have to synchronise their clocks with the Indian government’s Network Time Protocol (NTP) servers, maintain ICT system logs for 180 days, and implement know-your-customer (KYC) requirements for cryptocurrency exchanges and wallets.

The guidelines also mandate the adoption of cybersecurity policies and the appointment of a chief information security officer (CISO) by “certain entities”.

“Service providers, intermediaries, data centres, body corporate, Virtual Private Server (VPS) providers, Cloud service providers, VPN Service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and Government organisations shall follow these Cyber Security Directions of 28.4.2022 as applicable to them,” said the explainer issued by CERT-In.

The VPN policy, in discussion since April 2022, wanted operators to create user logs, maintain them, and hand it over to the government when asked. Most VPNs decided to move on rather than bow down.

“It is our policy to never allow logging, and we have also specifically designed our VPN servers to not be able to log, including by running in RAM. Data centers are unlikely to be able to accommodate this policy and our server architecture under this new regulation, and thus there is no path forward other than to no longer have physical VPN servers in India,” said Harold Li, vice President, ExpressVPN in a statement issued in response to the laws.

“We are a strict no-log company. While we do not collect any identifiable information from our users, we cannot operate physical servers in a country where we will be forced to change our operating methods and compromise our users’ privacy and security”, PureVPN marketing communications head Shaheryar Popalzai said in a statement.

Certain aspects of these guidelines pose a risk to India’s open, connected, secure, and trustworthy internet, as well as to global industry standards on cybersecurity practices, noted the Internet Society.

“Zero-knowledge systems enable security and anonymity over the Internet, discourage tracking and profiling and help keep users safe on the Internet, especially vulnerable and marginalized sections of society. CERT-In’s directions risk diluting the essence of these tools that keep all of us safe when we are online,” said an Internet Society report on the Bill.

“The directions were released by CERT-In without any public consultation with technology and cybersecurity experts, which has led to the inclusion of multiple unwarranted provisions,” said The Internet Freedom Foundation in its assessment of the rules.
Shape up or ship out

Singapore, which has been at the forefront of cyber regulations, tightened its control over the operations of cybersecurity companies.

The Cyber Security Agency of Singapore (CSA) implemented new regulations for cybersecurity service providers in 2022. According to the CSA statement, the move was to safeguard the interests of consumers and address the issue of information imbalance between consumers and providers.

Under the present norms announced in April 2022, the CSA will grant licences to those offering penetration testing and managed security operations centre monitoring services, including companies or individuals providing these services directly, third-party providers supporting such companies, and resellers of licensable cybersecurity services. All existing cybersecurity service providers had to obtain a licence or had to stop offering these services by October.

The licensing policy currently applies to managed security operations and penetration testing.

“These two services are prioritized because the CSPs performing these services have significant access to their client’s sensitive information, and if abused, will result in major disruption of the client’s operations,” noted the US International Trade Administration Office.

“In addition, these two listed services are already widely available and adopted in the market and thus could pose a significant risk to the overall cybersecurity landscape in Singapore.”

Currently, anyone providing licensable cybersecurity services without a licence could face a prison sentence of up to two years, a fine of up to S$50,000, or both.

“The licence is valid for a period of two years, and the licence fees for individuals and businesses are SGD 500 and SGD 1000, respectively. A one-time 50% waiver of the licence fees will be granted for all licence applications that are lodged within the first 12 months i.e. before 11 Apr 2023 to support businesses due to the impact of COVID-19,” the CSA announcement said.
Your data, your responsibility

Like Italy, Australia too was catapulted to the top slots of cybersecurity victims after the country offered support and solidarity to Ukraine against the ongoing Russian invasion.

Big-ticket cybersecurity incidents such as Optus and Medibank exposed sensitive personal and health information of millions, the Albanese government proposed to increase penalties for “serious or repeated breaches” of customer data.

The legislation raised the penalties for such breaches from the present $2.2 million to either $50 million or three times the value of any benefit gained from the misuse of information, or 30% of a company’s adjusted turnover during the relevant period – whichever is higher.

“When Australians are asked to hand over their personal data, they have a right to expect it will be protected. Unfortunately, significant privacy breaches in recent weeks have shown existing safeguards are inadequate. It’s not enough for a penalty for a major data breach to be seen as the cost of doing business,” said attorney general Mark Dreyfus in the government statement on the proposed legislation.

Australia home affairs and cybersecurity minister Clare O’Neil was noted for timely and proactive reactions to the continuous situations of crisis. She announced a collaboration between the Australian Federal Police and the Australian Signals Directorate: a 100-person team permanently focused on tracking and hacking the hackers.

“It will take some time to get this singing, but when it does, it will change the game for cyber in Australia,” she said at the annual press club address in December.
Cybersecurity Forecast for 2023
Paul Brucciani
CYBERSECURITY ADVISOR, WITHSECURE

Cryptocurrencies will be the focus of the most sophisticated and persistent attacks.

The inflationary forces welling up in economies running on ‘fiat currencies’ (i.e. paper-based promises to pay the bearer a certain amount, backed by the issuing bank) will be attracting increasing interest from investors. Cryptocurrency wallets and exchanges will be targeted by criminals and nation states.

The FAANGs will be in the dock

The FAANGs (Facebook, Amazon, Apple, Netflix, and Google) will come under increasing scrutiny by regulators around the world, for two reasons:

Cloud service availability: a large-scale, prolonged cloud service outage will raise questions about concentration risk

Market failure: AWS, Microsoft or Google will become embroiled in antitrust concerns as cloud service users become evermore dependent on the 3 service providers that control half the global market.

The digital world will become more fragile

The supreme irony is that the internet was created 40 years ago during the Cold War to overcome telecommunication vulnerability, yet today as geopolitical tensions rise, it has become a source to vulnerability. 90% of international internet traffic travels through just 436 submarine cables and if several lines are severed, there is very limited spare bandwidth to cope. Financial transactions worth over $10 trillion each day are done online, and any disruption would have an immediate effect on the economy, potentially crippling the banking system and halting commerce. The sheer volume of data cannot always be re-routed and would likely slow down or cripple activity across large parts of the web.

In the words of Henry Kissinger:

“Cables are easy to sever. 100 interruptions occur each year. Expect internet connectivity to come under threat in response to adverse geopolitical events.
If there is a ‘plan B’ worth having, it is, ‘How we will operate without the internet’.

Satellite communications will become a geopolitical target

Private satcom initiatives (e.g., Elon Musk’s Starlink network) will be viewed as trampling over longstanding international agreements about the exploitation of space, raising geopolitical tensions. When the geopolitical mode music is right, space powers will discuss creating a geospace treaty to bring order to how Earth-orbiting satellites are managed. Until then, they will be targets.

Competition in cyberspace, “is bound to threaten international order. It is difficult to assess national capabilities, vulnerabilities are multiplying, and there is no clear distinction between war and peace... We live in an age where “information has triumphed over knowledge and wisdom.”
Green computing

Cryptocurrencies like Bitcoin are digital money protocols that enable peer-to-peer transactions without the need of a central intermediary. Data mining is a computationally intensive way to prevent fraud and create trust among cryptocurrency users. The Bitcoin network alone, for example, uses as much power as an entire country like Malaysia or Sweden. Cryptocurrencies like Bitcoin will come under pressure to provide greener ways to maintain security.

The Ethereum Foundation says its switch from a ‘proof of work’ to ‘proof of stake’ verification method has led to a 100% reduction in energy for computation. Although it is a more environmentally friendly alternative to proof of work, it is also less secure.

Expect to see environmental regulation of computationally inefficient cryptocurrency service providers. Expect to see new forms of fraud based on subverting the ‘proof of stake’ security approach.
2023 EXPRESS FORECAST

Christine Bejerasco
CHIEF TECHNOLOGY OFFICER, WITHSECURE
5G and satellite connectivity will bring online new areas of the world

And this will have consequences: together with these come both positive opportunities for the most poverty-stricken areas, and opportunities for some of the people to go to a life of cybercrime. And there are no laws in those areas that would help curb this.

Reliable, ubiquitous connectivity enables more sustainable working patterns, reducing the carbon footprint of commuters and potentially improving our productivity.

The metaverse will dispel our remote working blues

The metaverse - a virtual-reality space in which users can interact with a computer-generated environment and other users - will increasingly be seen as an alternative to costly offices pinned to a single location. New techniques will be developed to communicate a profound, consistent understanding of complicated, multi-dimensional narratives. The metaverse will go some way to overcoming the limitation of online interaction.

Security will follow in the wake of these developments and until it catches up, it will be difficult to verify that participants are who they claim to be and the experience each person receives is authentic, and free from manipulation.

Cryptocurrency will be the fuel of Web3.

Once the initial madness regarding Web3 slowly gives way to real evolution, we can have real applications here.

Since this is 2025, I wouldn’t say that there are already wide applications here. But there should be a few mainstream applications that would need some real security. This could also be linked to the Metaverse, although that seems to be dominated by big tech today.
#1 – Cheaper GPUs means more potential for experimentation and increased crime-as-a-service development

The change of some of the cryptocurrency consensus (e.g. Ethereum making the transition from “proof-of-work” to “proof-of-stake” which is more eco-friendly) and the market being able to catch up with demand has resulted in dropped GPU prices. This means that more people will have access to powerful GPUs which can then be monetized. We will see increased experimentation as well as ML/AI that will be repurposed to criminal industries e.g. synthetic AI for written works and art. But also deep-fake generation for video, audio and handwriting; as well as things where ML/AI is already being used for anti-cheat systems for the online gaming world and to devise bypass mechanisms to bypass the detection ML/AI e.g. player pattern analysis. This means that companies should slowly but steadily start prioritizing integrity as part of the data assurance equation and start assuming that just because an image, conference call screenshot or even a written e-mail or signature looks legit, doesn’t mean it is. This means more pressure on PKI implementations or other cryptographic ways of establishing integrity and trust in order to avoid large scale phishing campaigns leveraging these kinds of novel manipulation methods.

#2 – Year 2038 is closer than we think. Strap in and start preparing

We are slowly starting to see Year 2038 problems with a few expected but also some unexpected impacts where technology plays a role. Anything where the year 2038 already plays a role e.g. calculating of termination dates of contracts, expiry dates of warranty on larger purchases or in the industrial world, etc. The first 2038 problems we will see today and in the next few years leading up to 2038 will have to do with planning, tasking, PKI and other systems where future dates have to be used. The media will make this a frenzy and might potentially blow it out of proportion, which is not necessarily a bad thing. In the case of Y2K, this was positive as it served as an awareness campaign because computers were fairly new to the mainstream population and the impact was limited because of the slow adaption but also because of the awareness. The issue is that the world runs on C/C++ today far more than it ran on COBOL in 2000, as basically all of our major operating systems, libraries and software eco-systems run on C/C++.

This is not something that will just pass us by. Companies will have to perform a non-cursory review of all software used as part of their core business processes, find out what vendors and manufacturers are doing to start having the dialogue to anticipate any potential problems. But also to make sure that processes are in place for reviewing the technology used by supporting services and third parties. Business continuity and disaster recovery planning will go up in the threat maps for most organizations, especially for those that have relied on smaller or bespoke software for which obtaining support is cumbersome, expensive or even impossible and for which alternatives will have to be sought and transitioned to.
#3 – Serendipitous convulsions towards a zero-trust IT estate, but not why you think

COVID-19 along with environmental constraints (can’t get to work because highway melted, hurricane, heatwave) and the current zeitgeist has transformed offices into open offices with “floating” desks. Open offices will continue to be unproductive but serendipitously it has led to the partial implementation of one of the zero trust principles which is that every seating location has the same privileges on the network: none (until proven otherwise with TPM/MFA/PKI after which *some* privileges are given based on the unique but temporary valid set of provided credentials).

The second big step is trying to help companies and the industry as a whole with their Active Directory addiction and trying to come up with alternatives that do not result in an “all or nothing” situation. Where even a partial compromise of Active Directory serving as the backbone IAM solution for the majority of organizations means a complete compromise of their digital estate and their data.

#4 – Tipping the scales, now with DDoS on top

Intercontinental disruptions such as fiber optic cable sabotage either on land or underwater will start becoming increasingly orchestrated in combination with DDoS/reflective attacks or a combination of the two. The latter we currently somewhat laugh away and blog/tweet about. Not so much when the backbone’s resilience is already under stress and companies are forced to make plans on an international disaster recovery basis. It is in these situations that impersonation, disinformation and other attacks become more prevalent when the normal methods of verification or integrity checking no longer work as there are less ways of reaching out and getting a second opinion or to verify claims.

#5 – Hybrid attack surface mapping remains an uphill battle for most companies that rushed their cloud transition/integration

Companies will continue to play catch up when it comes to knowing what their actual attack surface is, or what an attacker perceives as the attack surface relating to an organization. Especially with the introduction of so many different cloud services, the transparency levels have reached new lows of opaqueness to the point where companies are involuntarily down-prioritizing their own inventory assessment efforts and have to transfer the risk to their third parties and suppliers while for the most part betting on reactive controls such as detection and response.

#6 Unethical AI practices and AI abuse/misuse will increase while AI legislation is still being developed and debated

Use of unethical AI practices and the biases that come with them will continue and will only really be addressed when they start happening en masse or for incidents with larger impact. As some of the larger industries start making it mainstream, there will be more data and more potential for abuse/misuse. The EU AI act will help, but the real data about us historically, the apps we use and the data we have produced are not located, processed or monetized in Europe for the most part. Based on the above, we will have increased cases of “run away data” where on paper and for auditors the data is in a certain location but is enriched outside of certain legislated jurisdictions when it comes to ML/AI. In the same way that we currently do CO2 book-keeping to “buy clean air” from other countries, so too will there be an economy for data enrichment once the first legislation gets passed in certain regions of the world.

In the metal industry, companies spend millions shipping raw aluminum ore to Iceland because of the low cost of geothermal energy. So too will we have countries where data can be “shipped to” digitally, enriched and exported. The more moving parts and data, the more potential for misuse and abuse and thus leaks and real societal impact. The insurance industry along with special legislation will grow and be further introduced to the market to help manage the risk of data misclassification, prosecution and other data driven decisions coming from ML/AI. Systematic probing of AI/ML will become mainstream and detection for safeguarding AI algorithms will be required to protect the quality of outcome and data as well as detection of manipulation of the algorithms.
Social networks will continue to have the same problems they have today

Existing social network companies will continue to inadequately address disinformation, online harassment, and the problem that recommendation mechanisms lead many people towards belief in dangerous conspiracy theories and extremist views. YouTube will continue to be a vector for advertising scams, pushing harmful disinformation, and delivering malware. WhatsApp will continue to function as a good platform for delivering scams and malware. LinkedIn will continue to be an excellent tool for reconnaissance and social engineering attacks.

Adversarial machine learning attacks will still not be used in 2023

We first wondered whether havebeentrained.com was using membership inference attack methodology against image generation models. However, it turned out to be a simple similarity model derived from common training sets and their metadata. I still wouldn’t expect to see mainstream adversarial-machine-learning-attack-as-a-service operations in 2023.

“Trendy” large machine learning models will have little to no impact on cybersecurity

Large language models will continue to push the boundaries of AI research. Expect GPT-4 and a new and completely mind-blowing version of GATO in 2023. Expect Whisper to be used to transcribe a large portion of YouTube, leading to vastly larger training sets for language models. Despite the democratization of large models, their presence will have very little effect on cybersecurity, either from the attack or defense side. Such models are still too heavy, expensive, and not practical for use from the point of view of either attackers or defenders.

Natural language generation models will be used by adversaries

Children are already using natural language generation models to cheat on homework. Adversaries will start to use this technology to create convincing looking fake content. These models churn out grammatically correct, relatively well-written text that, at most, only require minor edits to become convincing and believable. Such methods could be used for the creation of fake NGO, think tank, and policy-related websites, fake company websites (in combination with thisstartupdoesnotexist.com) used in advanced and targeted social engineering campaigns, and fake social media profiles such as those used for targeted spear phishing on LinkedIn.
Shallow fakes will continue to reign over deep fakes

There will be further attempts to use DeepFakes for disinformation purposes, and more convincing videos will likely be created. However, shallow fakes – “screenshot tweets” that didn’t happen, doctored newspaper headlines, links to fake news articles, and misattributed videos will continue to be a more effective and widely used tool for disinformation.

New image synthesis techniques will be used to create fake social network avatars

Detecting that GAN-generated avatars were used to create fake social media accounts is currently a relatively trivial process, given that they are all generated by thispersondoesnotexist.com. A new site implementing the latest image generation techniques will be launched making it a lot more difficult to detect the use of synthetic images in fake social media avatars.

Alignment will bring the concept of adversarial machine learning into the public consciousness

AI Alignment is the study of the behavior of sophisticated AI models, considered by some as precursors to transformative AI (TAI) or artificial general intelligence (AGI), and whether such models might behave in undesirable ways that are potentially detrimental to society or life on this planet. This discipline can essentially be considered adversarial machine learning, since it involves determining what sort of conditions lead to undesirable outputs and actions that fall outside of expected distribution of a model. The process involves fine-tuning models using techniques such as RLHF – Reinforcement Learning from Human Preferences. Alignment research leads to better AI models will be discussed a lot more in 2023, and will likely become a mainstream topic, bringing the idea of adversarial machine learning into the public consciousness.

More attempts will be made to steal valuable machine learning models (via security breaches)

In late 2022, NovelAI, a company that provides ai art as a service was breached and their model leaked onto the Internet. As more and more services like this one start appearing, we might expect more models to be leaked or stolen, especially since most of those services charge their users for access.

AI-based voice mimicry will be used a lot more in high-value social engineering attacks

Voice mimicry technologies will become readily available and easy enough to use that we can expect their use to be more widespread in social engineering attacks.
Twitter users may move away from Twitter, but not to another social network

We may see a continued migration away from the current iteration of social networks. This could especially be the case if Twitter becomes yet another “haven for free speech” like gab, telegram, or parler under the leadership of Elon Musk. I see people on Twitter talking about returning to RSS feeds. Isolated discussion forums appear to be on the rise once again. If Twitter does become more of a toxic unmoderated hellscape than it is at present, there’s no real alternative for people to migrate to that serves the same purpose. This is a space that is ripe for a new social network that is able to solve some of the worst moderation problems exhibited by existing sites. However, an exodus of researchers, politicians, and journalists from Twitter may more likely precipitate a move away from the current social network model which will cause a shift in the disinformation (and perhaps cyber attack) landscape. If Musk cuts moderation efforts as he has indicated, we may see more unwanted content on Twitter, including porn, scams, disinformation, and malicious links. Hate speech and online harassment surged the day Elon purchased Twitter, in celebration of that action.

A change in the way cryptocurrencies are mined may change the motives of cybercriminals

Ethereum’s move away from energy-intensive, planet-destroying mining mechanisms may cause others to follow suit. This may change attackers’ motives, especially with respect to compromising cloud infrastructure to steal compute resources for mining purposes.

Privacy-invasive features may make their way into mobile games

Facial recognition libraries were found in early builds of Diablo Immortal, a game that was developed by Chinese company NetEase. China is very keen on collecting data of this kind. More mobile games coming out of China may implement gameplay functionality that encourages you to show your face.

Geospatial intelligence systems used in Ukraine may become the target of adversarial machine learning attacks

GIS Arta geospatial intelligence is a Ukrainian guidance command and control system for drone, artillery or mortar strikes that greatly reduces the decision chain around targeting processes. The system ingests intelligence from sources such as drones, GPS, and forward observers and converts it into dispatch requests for reconnaissance and artillery. The system utilizes machine learning mechanisms. The existence of this system may provide sufficient motivation for adversaries to craft attacks against its machine learning models and pipelines.
Russia will turn into a bandit state, also in cyberspace

Since the 24th February, Russia consistently turns into a state that has nothing to lose on the international scene. It is reasonable to expect that it will become a haven to cyber gangs and possibly even state-run ones. Currently, Russia has no incentive in limiting or prosecuting gangs attacking the “unfriendly states”. Some of state-sponsored activity can be masqueraded as hacktivism or independent cyber gangs. North Korea is a role model of such state-level activity.

When it comes to cybersecurity - detection and removal of the mining malware / software will become even more in demand.

Data processing emissions – an elephant in the sustainability room

We often forget that data transmission and crunching require a lot of energy. In 2021 it was around 600TWh of power and it excludes “the crypto” (https://www.iea.org/reports/data-centres-and-data-transmission-networks). Companies and individuals will seek for ways to decrease their emission footprint. One mitigation path is switching to renewable energy – many datacenters are already pretty advanced in doing so. What we can also expect is that there will be more and more emphasis on the energy efficiency of the software (code) and not just the infrastructure that runs that code. Because of the hiking prices or energy and cloud infrastructure, we can expect demand for more efficient software and the efficiency will likely become a competitive advantage. One of the most energy intensive jobs is the training of ML models. We can expect innovative ideas to optimize the energy footprint of AI technology application.

Cloud-specific attacks will become mainstream

Threat actors are becoming more proficient in cloud and cloud-specific attacks. So far, many of the attacks we see in the cloud are “ported” versions of traditional attacks. Threat actors benefit from the fact that currently cloud infrastructure is trickier to secure, monitor and control. Looking forward, we will see increasing number of attacks that are cloud-specific, utilizing specific cloud infrastructure weaknesses, misconfigurations and vulnerabilities. The complexity and variety of cloud IAM philosophies makes it especially hard to protect.

Simplification of cyber-defense over anything else

Increasing complexity of hybrid, multi-cloud environment is a fact and skills shortage is real. Companies and organizations want to protect all estates via a single pane of glass. The proper way to increase the security likely won’t be “one more system”, but a simplified ecosystem where the situational awareness would be provided by a single console.
Malware campaigns will move from human speed to machine speed. The most capable cybercrime groups will reach the capability to use simple machine learning techniques to automate the deployment and operation of malware campaigns, including automatic reaction to our defenses. Malware automation will include techniques like rewriting malicious emails, registering and creating malicious websites and rewriting and compiling malware code to avoid detection.
HACKTIVISM, DEEPFAKES, ATTACKS ON BUSINESS COLLABORATION TOOLS, NEW REGULATORY MANDATES, AND PRESSURE TO CUT COMPLEXITY WILL TOP ORGANIZATIONS’ SECURITY AGENDAS OVER COMING YEAR

C yberattacks across all industry sectors increased by 28% in the third quarter of 2022 compared to 2021, and Check Point predicts a continued sharp rise worldwide, driven by increases in ransomware exploits and in state-mobilized hacktivism driven by international conflicts. At the same time, organizations’ security teams will face growing pressure as the global cyber workforce gap of 3.4 million employees widens further, and Governments are expected to introduce new cyber-regulations to protect citizens against breaches.

In 2022 cybercriminals and state-linked threat actors continued to exploit organizations’ hybrid working practices, and the increase in these attacks is showing no signs of slowing as the Russia – Ukraine conflict continues to have a profound impact globally. Organizations need to consolidate and automate their security infrastructure to enable them to better monitor and manage their attack surfaces and prevent all types of threat with less complexity and less demand on staff resources.

Cybersecurity predictions for 2023 fall into four categories: malware and phishing; hacktivism; emerging Government regulations; and security consolidation.
Hikes in malware and hacking exploits

• No respite from ransomware: This was the leading threat to organizations in the first half of 2022, and the ransomware ecosystem will continue to evolve and grow with smaller, more agile criminal groups forming to evade law enforcement.

• Compromising collaboration tools: While phishing attempts against business and personal email accounts are an everyday threat, in 2023 criminals will widen their aim to target business collaboration tools such as Slack, Teams, OneDrive and Google Drive with phishing exploits. These are a rich source of sensitive data given most organizations’ employees continue to often work remotely.

Hacktivism and deepfakes evolve

• State-mobilized hacktivism: In the past year, hacktivism has evolved from social groups with fluid agendas (such as Anonymous) to state-backed groups that are more organized, structured and sophisticated. Such groups have attacked targets in the US, Germany, Italy, Norway, Finland, Poland and Japan recently, and these ideological attacks will continue to grow in 2023.

• Weaponizing deepfakes: In October 2022, a deepfake of U.S. President Joe Biden singing ‘Baby Shark’ instead of the national anthem was circulated widely. Was this a joke, or an attempt to influence the important U.S. mid-term elections? Deepfakes technology will be increasingly used to target and manipulate opinions, or to trick employees into giving up access credentials.

Governments step up measures to protect citizens

• New laws around data breaches: The breach at Australian telco Optus has driven the country’s Government to introduce new data breach regulations that other telcos must follow, to protect customers against subsequent fraud. We will see other national Governments following this example in 2023, in addition to existing measures such as GDPR.

• New national cybercrime task forces: More Governments will follow Singapore’s example of setting up inter-agency task forces to counter ransomware and cybercrime, bringing businesses, state departments and law enforcement together to combat the growing threat to commerce and consumers. These efforts are partially a result of questions over whether the cyber-insurance sector can be relied upon as a safety net for cyber incidents.

• Mandating security and privacy by design: The automotive industry has already moved to introduce measures to protect the data of vehicle owners. This example will be followed in other areas of consumer goods that store and process data, holding manufacturers accountable for vulnerabilities in their products.

Consolidation matters

• Cutting complexity to reduce risks: The global cyber-skills gap grew by over 25% in 2022. Yet organizations have more complex, distributed networks and cloud deployments than ever before because of the pandemic. Security teams need to consolidate their IT and security infrastructures to improve their defences and reduce their workload, to help them stay ahead of threats. Over two-thirds of CISOs stated that working with fewer vendors’ solutions would increase their company’s security.
Deepfakes will go mainstream with hacktivists and cybercriminals leveraging video and voicemails for successful phishing and ransomware attacks.

We will see a nation-state lead a sustained and lengthy attack against the USA’s power grid, leading to power disruptions impacting critical business and societal functions.

We’re entering a new era of hacktivism, with increasing attacks motivated by political and social causes. Threat actors are becoming increasingly shameless and will turn their attention to critical infrastructure.

Cloud transformation will slow due to cost and complexity, with many firms considering bringing workloads back in-house or to private data centres to reduce their overall threat surface.

Experts from Check Point, Exterro and Tenable share cybersecurity insights for 2023
The cyber insurance industry is undergoing major tectonic shifts. Companies will most likely not be able to rely on insurance as a safety net for cyber incidents. Like we’ve seen with the auto industry, policymakers will act to protect their constituents with legislation holding makers accountable for software defects that create cyber vulnerabilities. In turn, this will put the onus on software vendors to build in security validations.

Dan Wiley
Head of Threat Management, Check Point Software

While email and phishing go hand-in-hand and will still be dangerous and proliferate, in 2023 cybercriminals will also turn to business collaboration compromise, with phishing attacks used to access Slack, Teams, OneDrive, Google Drive, etc. Employees are often loose with sharing data and personal information while using these business apps, making them a lucrative source of data for hackers.

Jeremy Fuchs
Research Analyst, Avanan, a Check Point company

In our multi-hybrid environment, many CISOs struggle to build a comprehensive security program with multiple vendors. In 2023, CISOs will decrease the number of security solutions deployed in favor of a comprehensive, single solution to reduce complexity.

Jony Fischbein
CISO, Check Point Software

Dramatic increase of digital scams, due to a global economic slowdown and inflation. Cybercriminals will increasingly turn to social media campaigns via Telegram, WhatsApp and other popular messaging apps. There will also be more cyber-attacks on Web3 blockchain platforms, mainly to overtake platforms and their users’ crypto assets.

Oded Vanunu
Head of Products Vulnerability Research, Check Point Software
Hybrid work model will require smart digital forensics for in-house investigations

“India remains one of the most challenging economies when it comes to protection and enforcement of intellectual property. Coupled with the new hybrid work model, in house investigations have become doubly challenging as insider threat poses serious threat to businesses. When conducting a covert investigation, to detect if any user has been stealing proprietary information, it’s no longer a case of physically borrowing that laptop. Organizations need to obtain remote access to that device, scan and image it quickly. What Indian businesses need are digital forensics solutions that centralize data and analyze it so it can be sent to relevant investigative teams. These solutions will be a gamechanger in 2023 as businesses veer towards workflow automation to cut costs amidst turbulent economic conditions.”

If you think Ransomware is scary...

“Extortion will be an increasingly disruptive force to enterprises in all industries in 2023. In the past year, we’ve seen threat actors of all motivations moving to extortion-only attacks and forgoing the more complex tactics like data-encrypting malware (ransomware). The notoriety and success of extortion groups like Lapsus$ means that other groups will continue to mimic their tactics.”

Cryptocurrency scams will thrive in gloomy economic conditions

“In 2023, as economic conditions around the world remain uncertain, get-rich quick schemes involving fake cryptocurrency investments through social media and online dating will become increasingly successful, as worries about unemployment grow and the impact of inflation continues to affect consumers.”
More connections, more risk

“5G will usher in a new era of digital transformation in India. Coupled with increased IoT adoption, it opens up organizations to more risk than ever. This additional risk is especially relevant in industrial environments. Smart doesn’t necessarily mean secure and 5G adoption is expected to increase the attack surface as many IoT and IIoT devices have poor security implementations.”

Marty Edwards
Deputy CTO - OT/IoT, Tenable

OT spending will soar, even if IT spending stalls

“Challenging macroeconomic conditions will cause companies to reevaluate traditional IT cybersecurity spending, however these same companies will prioritize and proportionally increase security spending on their much more critical Operational Technology (OT) systems. The consequences of high profile events like Colonial Pipeline have demonstrated that the risk to OT is higher and boardroom cybersecurity discussions almost always include securing OT.”

Bob Huber
Chief Security Officer, Tenable

Big SaaS breach ahead

“I anticipate a significant breach of a SaaS provider in 2023. Given the adoption rates of SaaS applications, the shared responsibility model and limited monitoring, this attack surface is ripe for compromise.”

Dick Bussiere
Technical Director, APAC, Tenable

Data Privacy will change the way of doing business

“The new Digital Personal Data Protection Bill 2022, if enacted, will have a massive impact on businesses. In 2023, we will see Indian businesses begin adopting new technology and revising existing processes to keep up with the law. Organizations will gear up to conduct privacy impact assessments and we expect legal tech investments to increase. This is because businesses will need smart solutions to tackle the massive problem of knowing what data resides where, what to retain and what to delete.”

Rajkumar Manickam
Regional Sales Director, South Asia, Exterro
Cybercriminals will utilize AI and machine learning in 2023
1. Ransomware: Less encryption, more legislation

Ransomware and cyber extortion will remain among the top cyber threats in 2023. As cybercriminals’ tactics continue to evolve, they will increasingly favor exfiltrating data over encrypting it for cyber extortion. Governments will continue to strongly advise organizations not to pay ransoms and may even introduce legislation relating to this.

Double extortion ransomware (where a copy of the data is exfiltrated before it is encrypted) has surpassed traditional ransomware as cybercriminals’ extortion tactic of choice. The threat of the exfiltrated data being leaked provides cybercriminals with a secondary lever with which to apply pressure on victims to pay up. However, as organizations adopt stronger backup and resilience measures, the primary impact is now being caused by the data exfiltration, rather than data encryption. This may lead to some cybercriminals forgoing encryption entirely and refocusing on exfiltration efforts. There have already been notable cases of ransomware which either skipped or faked data encryption.

Governments will continue advising organizations against paying ransoms to prevent financing of criminal organizations. The UK’s Information Commissioner’s Office (ICO) and National Cyber Security Centre (NCSC) released a joint letter to lawyers in June 2022 clarifying that UK “law enforcement does not encourage, endorse nor condone the payment of ransoms” although “payments are not usually unlawful”. As ransomware continues to rise, governments around the world may go a step further and introduce legislation to prohibit ransomware payments.

2. Phishing: Powered by AI

Machine learning and artificial intelligence have quickly become key technologies in the fight against cyber threats, for example, helping businesses to detect attacks by monitoring network patterns and analyzing anomalies or malicious behaviors. However, as AI has become more advanced and accessible, it has also been adopted by cybercriminals.

Cybercriminals will utilize AI and machine learning in 2023 to power more sophisticated phishing campaigns. Cybercriminals will have access to an ever-growing treasure trove of data, from open-source data such as job postings to personal information leaked in data breaches, with which to craft highly targeted spear phishing lures. Researchers have already shown how next-generation language models such as OpenAI’s GPT-3 can be used to generate phishing content that “outperformed those that were manually created”. With GPT-4, the next evolution of the language model, rumored for release in 2023, the threat of AI powered phishing becomes more severe.

3. Hacktivism: From nuisance to damaging

As the barrier to entry for cyber-attacks continues to drop, organizations will have to contend with a rising threat of hacktivism. Political, ideological, and social activists will increasingly use cyber-attacks as a vehicle to promote their causes, cooperating with other threat actors to launch more damaging attacks.

Interest in hacktivism rose over 2022 due to high profile geopolitical and social issues. A prominent example of this was the IT army of Ukraine, a hacktivist cyberwarfare group created in response to Russia’s invasion of Ukraine, which has conducted thousands of cyber-attacks against Russian assets.
Cybercrime-as-a-service offerings will help to bridge the capability gap between hacktivists and more mature threat groups. Compromised accounts, customized malware, botnets, and phishing kits easily purchasable on underground forums or private messaging channels and can be used to launch sophisticated cyber-attacks. We expect hacktivists to supplement their current arsenal of primarily distributed denial of service (DDoS) and defacement attacks, with large scale data exfiltration, encryption, or deletion.

1. Emerging technologies: Web3 and IoT

The Internet of things (IoT) is one of the bigger emergent technologies, which can affect everybody, especially with digitalization of every aspect of modern life. IoT devices are being deployed everywhere, from home networks to industrial and corporate networks. The number of connected IoT devices is expected to reach over 14 billion by the end of 2022 and continue growing in 2023. If secured incorrectly, these devices can offer substantial security risks and are often the target of brute force password attacks, DDoS or Person in the Middle Attacks (PitM).

In 2023, we will also see further use of Web3 technology and the deployment of centralized applications which promise increased security, reduced energy costs, increased privacy and greater control. Web3 developers will attempt to minimize the need for complex code, allowing inexperienced coders to build Web3 applications. However, as Web3 usage grows and new products and services are built on the technology, cybercriminals will look to take advantage of the hype and strike while the Web3 space is still relatively immature from a security perspective. Financial applications of Web3 technologies such as cryptocurrency will continue to be heavily targeted by cybercriminals, with more notable attacks to come against crypto exchanges.
Payment systems worldwide are under increased pressure to mitigate risks of fraud and to defend against persistent attacks from criminals who continue to grow in sophistication. As businesses continue on their digital transformation journey’s, cyber risk becomes an ever-prevalent concern. It certainly keeps me awake at night, as I am sure it does every senior leader in our industry. Minimising payment fraud is a strategic priority for both GPS and our customers worldwide who put the protection of their cardholders’ accounts first and in 2023, I expect we will see companies investing more in their risk management capabilities.

As always in the payments space, every player must remain keenly aware of the regulatory landscape in all the markets in which they and their customers operate. This climate can produce both growth tailwinds and debilitating headwinds, depending on the issue. In particular, we can expect data privacy, the stability of the crypto market and BNPL to continue to command the attention of legislators. The smartest players will not just track the regulatory landscape, but get ahead of it and shape it too. Companies like Zilch, which take a proactive approach to guidance and compliance, will be rewarded for that behaviour.
Four Trends Set to Define Cybersecurity in 2023

2022 was a challenging year for enterprise security, with consumers losing trust in businesses’ ability to keep their data safe. More than a third (35%) say they don’t trust any company to adequately protect their data, while nearly half (45%) have stopped, or would stop, using a company’s services following a serious data breach.

On top of this, the complexity of companies’ IT environments continues to grow. In particular, APIs - one of the foundational pillars of the modern internet - are increasingly under assault. API insecurity costs organizations up to $75 billion a year and is expected to rise as the number of APIs in use rises. So, with consumer trust falling and the challenge facing IT teams becoming ever more difficult, Imperva predicts that 2023 could be a challenging year ahead for the industry. Here are four key trends set to define 2023 according to Imperva’s experts:

The extinction of mainframes will accelerate as organizations data will be put at increased risk

Most popular game developers collect data, including the user’s personal information, real names, email addresses, cities and countries, and even the language they use. Nevertheless, many online game producers list their privacy policies to the public, detailing how they collect data and how it is used, in contrast to customary business procedures.

Many governments, especially those in the American and European continents, demand businesses disclose the data they are gathering and the purposes for which it is being used.

Ron Bennatan
General Manager Data Security at Imperva
An organisation will receive a record fine because it was using a patchwork of security tools to protect its data

Too many organizations still tackle data security with a patchwork of technology, leaving most data unmonitored and unprotected. At the same time, regulations continue to expound on the need for specific types of monitoring and protection for different types of data, further exacerbating the risks of siloed security practices. 2023 will see a huge wake-up call as at least one organisation will receive a record fine because of its lack of unified security.

On average organizations are juggling more than 75 security solutions across network, application and data security. Trying to manage these tools increases both the risk of burn-out and the chance that security teams will miss threats. With new threats to data, applications and networks emerging all the time – from increasingly sophisticated API attacks to fresh bot exploits – organizations will need a unified approach to stand a chance of tackling these new dangers, avoiding hefty fines, and protecting their most sensitive assets.
Bots will take over the internet and learn to target APIs

By the end of 2023, half of all internet traffic will not come from a human. What’s more, two-thirds of all bad bot traffic will be considered moderate or advanced, making these automated threats harder to detect and stop. In 2023, APIs will become the prime target for bad bots. Seen as signposts to sensitive data, 2022 saw vulnerable APIs cost businesses $75 billion a year. This problem is only going to worsen in 2023 as API defences often overlook automated threats.

Bots will become a persistent threat that organizations need to look out for or risk data leakage. The challenge is that tried-and-tested methods of defeating bots may not work. For instance, returning a CAPTCHA challenge to an API request breaks the calling application. Businesses need to use machine learning to differentiate normal API behaviour from malicious traffic, and to understand what data should be transmitted through the API. Organizations will face an uphill battle mitigating automated attacks targeting their API libraries until bot management and API security are used correctly.
Organizations will realise bundled cloud security tools aren’t fit for purpose

2023 will be the year we see organizations begin to question whether they are being too trusting of cloud security. They will increasingly realise that the cloud is not secure-by-design and that bundled security tools from cloud providers simply don’t cut it. Despite initially appearing to be easy to use, enterprises are finding – to their cost – that the one-size-fits-all approach of many cloud services’ security offerings simply cannot fully protect data in the cloud. There will always be differences in circumstances that leave a gaping hole for attackers.

Without putting in proper controls to secure the cloud, vulnerabilities and misconfigurations of cloud environments will be one of the biggest risks to data. Enterprises will see a thorough security audit as one of the essential steps to adopting any cloud service and ensuring that they have the right security and tools in place to meet their exact needs, instead of blindly trusting their provider. After all, it doesn’t matter how much money you save migrating to the cloud if you increase the risk of a costly breach in the future.

Andy Zollo
Vice President EMEA at Imperva
Adopting a Different Way of “Cyber-Thinking” in 2023

- By Luke Secrist, CEO, BuddoBot

This year endured a decent dose of cyber-immaturity slaps across the face. According to McKinsey & Company, at the current growth rate, damage from cyberattacks will amount to about $10.5 trillion annually by 2025 – a 300% increase from 2015.

Over the last several years, in the run-up to the new year, threats, attacks, and scams have risen, and that won’t be different in 2023. But the devil is in the details. Here are five trends we’ve seen and expect to proliferate:
1. **Increase in Cyber Threats and Malicious Attacks.**

More criminal organizations will use cyber force to target critical infrastructure and operational technology. The level and breadth will be inconspicuous such as hacking transportation devices (i.e., streetlights) or hospital monitoring systems. With recent upticks in malicious attacks against hospitals and patient care establishments, cybercriminal actions can be especially damaging. Such attacks render trickle-down damage not only to the organization under attack but also to the patients at the mercy of the locked-down IT systems. In one incident, a hospital’s digital tools were taken down by ransomware, causing patient overdoses. In another, our team was able to gain access from an uncredentialed network into the ICU at a leading hospital and took control of their life support systems.

2. **Risks from Machine Learning Adaptation.**

Learning (ML) will become more of a commodity, and threat actors will leverage both to improve attack scale, success, and effectiveness. We expect an increase in advanced phishing attacks targeting users across applications. Using AI and ML to automate tasks, cybercriminals will build employee maps by “crawling” social networks using algorithms to create automated emails. We’ve deployed sophisticated phishing attacks with over 75% success rate – add AI and ML to automate deployment and the odds of success increase.

3. **More People on the Internet = More Likelihood of Cyber Threats.**

Internet dependence is not a new concept but a new reality. By 2025, more than 91% of people in developed countries and 69% in emerging economies will use the Internet. Increased access exposes people and devices to more threats, and when development environments speed up, security often isn’t top of mind. We’ve seen first-hand organizations invest in solid perimeter security appliances and not configure them properly. When we throw threats at a network, it should light up appliances, but we’ve seen zero response.

4. **Crypto Threats are Growing and Evolving.**

Phishing attacks with domain spoofing, malicious browser extensions, and malware that scans for crypto wallet passphrase keys have seen success in the last five years. As companies adopt cryptocurrency/payments, scammers will target crypto wallets and personal information. Companies selling NFTs with IPs, that many users want to buy, will put them at increased risk. Web3 has seen many unique attacks, but it is still built on Web2 technology, creating concern about attack surface potential. You can’t secure your Web3 infrastructure if Web2 is susceptible.
5. **Breach Recovery Will Cost More.**

If cybercrime were measured as an economy, it would be the world’s third-largest after the U.S. and China. Attacks show no signs of slowing down. New tactics to siphon money are trending. Files are stolen from victims before encryption and threats to leak them on the dark web ensue. This “double extortion” method incentivizes victims to pay ransom even with a secure backup. Destruction of data, stolen money, theft of IP, personal and financial data, embezzlement, fraud, post-attack disruption to business, forensic investigation, restoration of hacked data and systems, and reputational harm are only some of the consequences.

Organizations need to consider these trends to improve their cybersecurity posture. But how? It starts by thinking differently.

6. **Bolster your defense with offensive cybersecurity.**

Defense is one part, offense the other. Start with a conversation about issues and roadblocks. It’s better to uncover and discuss gaps than be breached. A strong defense is important but not enough. Most organizations question spending beyond compliance. Defense-based appliances, MSPs, and blue teams are critical; however, validating that the defenses work is equally necessary. You will never know susceptibility unless you simulate real threats.

7. **Deploy Continuous Threat Simulation with Planned and Unplanned Attacks.**

Companies testing once a year for compliance are missing the point – it’s not enough. You need a continuous testing model that includes at least a dozen external tests each year, most of which should be unplanned. Hackers don’t work around your schedule. Consider how your organization will do with its guard down.

New threats will persist. Don’t ignore cyber-hygiene or validating your defense through strong offensive threat simulation. It’s like flossing your teeth. We know it’s important, yet most don’t do it. Avoid cyber-gingivitis and preventative care will never look the same.

---

**Luke Secrist**

CEO at BuddoBot

A veteran of the U.S. Marine Corps, Luke Secrist began his career in military defense contracting as an IT security engineer and systems manager. While working for companies of different sizes, his desire to start a cybersecurity business of his own grew. He envisioned a commercial startup that would cultivate subject matter expertise and creativity in a structured yet deconstructed environment. He realized this dream in 2008 with BuddoBot, a cybersecurity firm that takes an offensive (vs. defensive) approach to protect its customers’ IT systems from bad actors. The company name is a combination of “Buddo” (a derivative of buddy) and “Bot” (a representation of technical efficiency and accuracy), reflecting Secrist’s friendly and team-oriented style to providing professional services. It also symbolizes an organizational culture driven by the desire to learn and think outside the box to help people mitigate real threats. BuddoBot serves an extensive list of clients in the federal government, healthcare, manufacturing, financial services, education, and other industries.
Malware-as-a-Service on the rise, ransomware rotates away from Bitcoin: a look at crimeware and financial threats in 2023

In 2023, we will observe a great demand for malware loaders on the darknet: instead of developing their own malicious samples, attackers will opt for ready-made services with enhanced detection avoidance. Moreover, due to increasing regulations imposed on cryptomarkets, crimeware gangs move away from Bitcoin seeking other forms of value transfer. These are the key predictions from Kaspersky’s ‘Crimeware and financial cyber threats in 2023’ report.
As the financial threat landscape has been evolving dramatically over the past few years, Kaspersky experts believe it is no longer sufficient to look at the threats to traditional financial institutions, but that it is better to assess financial threats as a whole. The cybercrime market has been developing extensively, with the overwhelming majority of attackers pursuing one goal – financial profit. This year, our researchers have decided to adjust their predictions accordingly, expanding them to encompass both crimeware developments and financial cyberthreats. By analyzing the significant events and trends that formed both crimeware and the financial threats landscape in 2022, our security experts and researchers have forecasted several important tendencies expected in 2023. Here are their key prediction
• **Led by gamers and other entertainment sectors, web3 continues to gain traction and so will threats to it.**

With the increasing popularity of cryptocurrencies, the number of crypto scams has also grown. However, users are now much more aware of crypto and will not fall for primitive scams such as the dubious cryptocurrency scheme that went viral featuring a video with a deepfake “Elon Musk”. Cybercriminals will continue to try stealing from people using fake ICOs and NFTs, and other cryptocurrency-based financial theft. Along with the exploitation of vulnerable smart contracts, criminals will use and create more advanced methods to proliferate their crimes.

• **Malware loaders are to become the hottest goods on the underground market.**

Many actors have their own malware, but that alone is not enough. Entire samples used to consist of ransomware alone. But when there are different types of modules in ransomware, it is easier for the threat to evade detection. As a result, attackers are now paying much more attention to downloaders and droppers, which can avoid detection. This has become a major commodity in the Malware-as-a-Service industry, and there are already favorites among cybercriminals on the darknet, for example the Matanbunchus downloader. All in all, stealth execution and bypassing EDR’s is what malicious loaders developers are going to focus on in 2023.

• **More new penetration testing frameworks will be deployed by cybercriminals.**

While various vendors create and improve penetration testing frameworks to protect companies, such as Brute Ratel C4 and Cobalt Strike, crimeware actors are expected to use them much more actively for illegal activities. Along with the development of new penetration tools, cybercriminals will increasingly use the frameworks for their own malicious purposes.
• **Ransomware negotiations and payments will rely less on Bitcoin as a transfer of value.**

As sanctions on ransomware payments continue to be issued, the markets become more regulated, and technologies improve at tracking the flow and sources of Bitcoin (and sometimes clawing back conspicuous transactions), cybercrooks will rotate away from this cryptocurrency and toward other forms of value transfer.

• **Ransomware groups following less financial interest, but more destructive activity**

As the geopolitical agenda increasingly occupies the attention not only of the public but also of cybercriminals, ransomware groups are expected to make demands for some form of political action instead of asking for ransom money. An example of this is Freeud, brand-new ransomware with wiper capabilities.

“We are predicting two major scenes inside the ransomware landscape in the upcoming year. One of them will be the usage of destructive ransomware with the unique purpose of resource destruction and the impact of what we call ‘regional attacks’, where certain families only impact certain regions. For instance, the mobile malware landscape made a big evolution in Latin American region, bypassing the security methods applied to banks such as OTP and MFA. The Malware-as-a-service is another important thing to observe as this kind of underground service is commonly observed around ransomware attacks impacting larger organizations,” says Marc Rivero, a senior security researcher at Kaspersky’s Global Research and Analysis Team.
The shifting cybersands: Threat landscape insights and predictions for 2023

According to Kaspersky Security Network statistics, about every third user in the META region was affected by online and offline threats in January-September 2022. Focusing on the Middle East, Qatar had the highest number of users affected by online threats (39.8%). Followed by Bahrain (36.5%), Saudi Arabia (33.3%), UAE (32.9%) and Kuwait (32.5%). Fewer users were affected in Egypt and Jordan (28.1% and 28% respectively).

The highest numbers of offline threats in the Middle East were reported in Egypt (42.4%), Qatar (33.9%), and Jordan (33.2%). Bahrain (32.4%), UAE (32.3%), Kuwait (32.3%) and Saudi Arabia (32%) had the lowest numbers of affected users in the Middle East by local threats.
Today’s hyper-connected world requires us to reconsider the way we do cybersecurity. We need to shift toward a more reliable approach – one with no room for error. This is why we’re working on developing Cyber Immune products with “innate” protection against cyberthreats. Most attacks on the Cyber Immune systems are ineffective. It’s through events like this one in Jordan that we’re able to share our innovations and educate our audience about a safer and more resilient digital world where Cyber Immunity is the new norm,” said Eugene Kaspersky, CEO of Kaspersky.
INCREASE IN APT INTRUSIONS IN THE META REGION

In 2022 there has been an increase in the number of persistent and sophisticated attacks targeting various states in the META region. Starting from the most recent threat actor Metador targeting telecommunication companies, HotCousin expanding its operations to this region, the numerous campaigns deploying various IIS backdoors, DeathStalker and Lazarus attacking multiple industries there and a mysterious SSP-library backdoor discovered on governmental and non-profit entities, there were several new threats active in the region over the last year.

2023 predictions – what’s next?

The 2023 forecast is based on Kaspersky expertise and the activity witnessed this year while tracking more than 900 APT groups and campaigns.
The next WannaCry and drones for proximity hacking.

Statistically, some of the largest and most impactful cyber epidemics occur every six to seven years. The last such incident was the infamous WannaCry ransomware worm, leveraging the extremely potent EternalBlue vulnerability to automatically spread to vulnerable machines. Our researchers believe the likelihood of the next WannaCry happening in 2023 is high. One potential reason for an event like this occurring is that the most sophisticated threat actors in the world are likely to possess at least one suitable exploit, and current global tensions greatly increase the chance that a ShadowBrokers-style hack-and-leak could take place. Major shifts will be reflected in new types of targets and attack scenarios too, as experts believe next year, we may see bold attackers become adept at mixing physical and cyber intrusions, employing drones for proximity hacking. Some of the possible attack scenarios include mounting drones with sufficient tooling to allow the collection of WPA handshakes used for offline cracking of Wi-Fi passwords or even dropping malicious USB keys in restricted areas in hope that a passerby would pick them up and plug them into a machine.

Other advanced threat predictions for 2023 include:

- **SIGINT-delivered malware.** One of the most potent attack vectors imaginable, which uses servers in key positions of the internet backbone, allowing man-on-the-side attacks, may come back stronger next year. While these attacks are extremely hard to spot, our researchers believe they will become more widespread and will lead to more discoveries.

- **The rise of destructive attacks.** Given the current political climate, Kaspersky experts foresee a record number of disruptive and destructive cyberattacks, affecting both the government sector and key industries. It is likely that a portion of them will not be easily traceable to cyberattacks and will look like random accidents. The rest will take the form of pseudo-ransomware attacks or hacktivist operations to provide plausible deniability for their real authors. High-profile cyberattacks against civilian infrastructure, such as energy grids or public broadcasting, may also become targets, as well as underwater cables and fiber distribution hubs, which are challenging to defend.

- **Mail servers become priority targets.** Mail servers harbor key intelligence, making them valuable to APT actors, and have the biggest attack surface imaginable. The market leaders in this industry have already faced exploitation of critical vulnerabilities, and 2023 will be the year of 0-days for all major email programs.

- **APT targeting turns toward satellite technologies, producers and operators.** There is evidence of APTs being capable of attacking satellites, with the Viasat incident as an example. It is likely that APT threat actors will increasingly turn their attention to the manipulation of, and interference with, satellite technologies in the future, making the security of these technologies ever more important.

- **Hack-and-leak is the new black.** The new form of hybrid conflict that unfurled in 2022 involved a large number of hack-and-leak operations. These will persist in the coming year with APT actors leaking data about competing threat groups or disseminating information.

- **More APT groups will move from CobaltStrike to other alternatives.** CobaltStrike, a red-teaming tool, has become a tool of choice for APT actors and cybercriminal groups alike. It has gained significant attention from defenders, making it likely that attackers will switch to new alternatives such as Brute Ratel C4, Silver, Manjusaka or Ninja, all offering new capabilities and more advanced evasion techniques.
With a focus to create awareness and build an unwavering cybersecurity network, infosec publication The Cyber Express launched the India Edition of World CyberCon 2022. The one-day event took place on November 18, 2022, at Courtyard Marriott, Mumbai.

The cybersecurity event witnessed an exchange of ideas from like-minded cybersecurity enthusiasts from industry, academia, and government on topics such as Zero Trust Architecture, the Future of Multi-Factor Authentication, and the need to look beyond the traditional compliance-based security awareness.

A proud event for the news service, the conference witnessed the launch of our print edition. The 85-page paperback had exclusive interviews of cybersecurity leaders and deep-researched feature reports on important and interesting developments in the sector. The magazine proved to be an instant hit among the speakers as well as the delegates.

The conference started with an authoritative speech by keynote speaker Brijesh Singh, the Additional Director General for police in Maharashtra, who shared invaluable professional insights about the gap between cybercrime and the current cybersecurity laws. Among the series of insightful, informative, and interactive speaker sessions, panel discussions, and fireside chats that followed, the panel discussion on the role of women in cybersecurity attracted particular attention.
PARTICIPATING COMPANIES

- **C-Suite/President**: 55%
- **VPs/Directors**: 15%
- **Heads**: 10%
- **Managers/Senior Managers**: 15%
- **Others**: 5%
Aces of Cyber Spades

TOP 10 GUARDIANS OF CYBER SPACE IN 2022
We at The Cyber Express are honored to acknowledge the effort and commitment of all those in the cybersecurity field who work tirelessly to protect our companies and our communities from cyber threats.

However, with so many highly skilled cybersecurity experts worldwide, selecting the top 10 was an uphill task. Hence, we conducted a poll to choose the Top 10 Guardians of Cyber Space in 2022.

Here are our Cybersecurity stalwarts who are on the front lines of cybercrime prevention, setting a benchmark for excellence in cyberspace. These individuals are dedicated to protecting our online safety and security, and we are grateful for their tireless efforts and expertise.
David B. Cross is the senior vice president, and the chief information security officer at Oracle, Washington. He is an expert in next-generation SIEM, incident response, and cloud red team endeavors. Previously, David worked as a venture partner at Rain Capital for over four years and as a freelancer at Team8 where he exchanged ideas with a global community of cybersecurity senior executives, CISOs, and thought leaders.

David was a member of Aphinia, an angel investor at Toucan, an investor at POSaBIT, and an owner at Cross Property Investments, LLC. Furthermore, he was a seed investor at Twistlock and an investor at PlaceFull. He was an engineering director of a public cloud security platform for Google, and the general manager for cloud and enterprise security, among other positions at Microsoft, for over 15 years.

He served in the US army as the HHC 81st brigade between 2000 and 2003 and also worked at the prestigious US navy in the VAQ-130 electronic attack squadron for over five years. He was awarded several medals for his selfless work in the area of overseas combat missions. He did his Bachelor of Science from the Chapman University and Master of Business Administration from City University.

David has been a volunteer and a founding board member at the VALA: Venues for Artists in the Local Area. He has earned over 50 licenses and certifications, including the DDoS attacks and Defenses certification from the University of Colorado. He was among the winners of the top 50 information security professional award, Chapman University distinguished alumni award and earned several medals issued by the United States Navy, NATO, Marine Corps, and Southwest Asia Service.
Abid Adam is the group chief risk and compliance officer at Axiata for over 5 years now. He was a freelance professor at Deakin University and served here as an adjunct professor and executive advisory board for cybersecurity. He was featured in the top 100 global CISOs in 2020 and has been an esteemed keynote speaker.

He worked as a freelancer executive member at CyberEdBoard community and was a chief information security officer at Old Mutual Limited before that. Abid worked at the Standard Bank South Africa where he joined as the head of information risk management and contributed towards leading and defining the information security governance forums and processes. He also helped establish the information security management and IRM functions and contributed to the company being promoted to the technology risk and business information security officer’s role.

Abid shouldered the responsibility of the business continuity and information risk manager at the Standard Bank of South Africa for over four years. He was the information security consultant at Secure Data before that. Abid is a certified data privacy solutions engineer from ISACA and has earned leadership in the digital age and business administration from INSEAD.

He has the CISSP certificate from ISC2, PCIRM from Ultima Risk Management, and risk management certification from Carnegie Mellon University – Heinz college of information systems and public policy, among other certifications.
Mathieu Lahierre works in the principal, application, and data security area at BHP. He was a part of the APAC data leakage prevention as a project manager and vice president between 2015 and 2017. He extended his knowledge at the Societe Generale Corporate and Investment banking for over four years in several positions. Such as the information security consultant in 2010, the project manager in 2013, and the process manager thereafter.

Mathieu was an information security consultant and competitive intelligence analyst, Paris, France at the Chambre de commerce et d’industrie de région Paris Ile-de-France. Before that he worked as the economic attaché at the Ministère des Affaires étrangères et du Développement international. He served both its El Manama office and Nairobi office.

He served as a financial controller at E. Leclerc in Paris. Mathieu completed his bachelor’s degree in US Culture and Business from UC Santa Barbara and a master’s degree in Management and Finance from ISEG. He further did his Master of Business Administration from Ecole de Guerre Economique in 2005.

He has over 30 licenses and certifications, namely the SSE expert certification, the insider threat program management, the CERT insider threat program manager, purple teaming, and the certified information privacy technologist from IAPP. Furthermore, he is a certified GDPR data protection officer and a certified blockchain security professional, among others.

Mathieu volunteered as a team leader for SAMU social emergency service for over seven years and as the deputy officer in the logistics for first aid units in the disaster and humanitarian relief area.
Holly Foxcroft
Head of Neurodiversity at Stott and May Consulting

Holly Foxcroft is the head of neurodiversity in cyber research at Stott and May Consulting. She was a lecturer for cybersecurity at Chichester college and was self-employed at NeuriDiversity Consultant, which had her work for the betterment of autistic staff and a universally inclusive work culture.

She was a part of the STEM apprenticeship executive and cybersecurity lead at Highbury college where she supported equality and diversity and worked closely with UK businesses and SMEs. Before that, she worked as an Incident response recruitment consultant, which involved resourcing candidates with incident response certifications.

She served the United Kingdom’s Royal Navy for over 6 years. Holly finished her bachelor of BSc, in criminology and cybercrime, from the University of Portsmouth. She was featured among the most inspirational women in cyber-UK 2020.

Holly passionately works in the area of creating policies and mentorship for neurodiversity in workplaces. She seeks to create a transformation in the culture to create more acceptance and reduce biases at work. She is a supporter of neuroinclusive work environment, which according to her, should be universal by design. She advocates a top-down approach to thwart the presently biased work scenario.

She is also working with five core partners with engagement workstreams and has the vision to create a strong base of cybersecurity staff and increase the core partnerships beyond the present consulting packages.
Jay Hira
Director of Cyber Transformation, EY

Jay Hira is a cybersecurity transformation director with over 15 years of experience in zero trust principles, business-aligned cyber resilience strategies, and building revenue security while maintaining customer trust.

He works as the director of cyber transformation at EY and has been self-employed at MakeCyberSimple. Jay has been a guest lecturer at the prestigious University of New South Wales, Australia. He lent his expertise as a security and compliance auditor at Salesforce and was a senior manager for cybersecurity at EY between July 2018 and August 2020.

Jay shouldered several responsibilities at various firms, such as QBE, where he was a project manager, Accenture as a security and risk manager, and IBM as the senior consultant. He was the senior advisor at KPMG and started off his career as an associate consultant at Wipro in 2007. He completed his master's program in network technology and IT infrastructure from Symbiosis center for information technology.

He was awarded the cyber personality of the year award and cyber security influencer for the year 2022 by Cyber security awards. Jay has contributed generously to causes revolving around education and has volunteered as a student mentor at three prestigious organizations, including the business information systems association, the UNSW sandbox program, and UNSW women in technology. At ISACA, he volunteered as a course instructor and was a founding board member and director of the ISC2 Sydney chapter for over five years.
Brian Krebs
American journalist and investigative reporter

Brian Krebs is a staunch follower of internet security and has been writing relentlessly for over 20 years, creating a stir in the infosec industry. He presently works at KrebsOnSecurity where he has been writing for over 13 years as a reporter and publisher of internet security and cybercrime news. He has authored a book named Spam Nation: The inside story of organized cybercrime, from global epidemic to your front door.

Krebs worked for 15 years at the Washingtonpost.com from 1995 to 2009. He has been honored with several awards, such as the cybersecurity person of the year award by CISO mag and the president’s award for public service that was issued by the information systems security association (ISSA). He has been bestowed with the media and cultural studies award by the Association of American publishers, the PROSE award for his book spam nation, and also the chairman’s citation in 2015 by the National Press Foundation.

Brian received the guardian award from the association of certified fraud examiners, the best blog post of the year, the most educational security blog award, the Mary Litynski award, and the best non-technical security blog, among others. He studied political science, and international relations from the George mason university in 1994.
Kris Lovejoy is the global security and resilience practice leader at Kyndryl. She made stellar contributions as a global cybersecurity leader at Ernst and Young and was the chief executive officer at BlueVector, Maryland. She was also the founder and CEO of BlueVector Inc, which worked with the AI-powered sense and response platform.

Kris was the president at Acuity solutions and served at IBM, starting as the VP of security strategy for three years, followed by the VP for IT risk/ CISO, and then the GM for OBM security services division for over four years.

As a leader in cybersecurity, she extended her knowledge of consul risk management as the CTO, CIO, and VP of support and services. Prior to that, Kris worked as the VP of security assurance services at TruSecure for five years. Kris has expertise in security, risk, compliance, and governance and was featured in the top 25 CTO in the InfoWorld list. Moreover, she was among the top 25 most influential security executives by the Security magazine and was among the top woman in security by eWeek.

Kris has the United States and European Union's patent for object-oriented risk management models and methods. She was named the top woman technology leader by Consulting magazine in 2020.
Celia Mantshiyane is currently the CISO at MTN South Africa. She was the group chief information security officer of Coca-Cola Africa and worked as a senior manager of IT infrastructure and operations at Sasria SOC limited.

Celia was the acting senior manager at the auditor-general of South Africa, where she would oversee several tasks, including a program of business change for the ICT department at Auditor general. She joined as the acting senior manager, where she extended her support to several projects in a span of six months and then worked as a business unit manager for another four years.

As a financial accountant at SABC in the Mmabatho area, South Africa, Celia performed managerial duties and contributed to SABC’s commercial and strategic planning for over 6 years. She started her career as a financial officer at Sebowane in 2005, where she handled creditor duties, monitored debtor activities, and took care of GL reconciliations, among other tasks. She also has experience in the TV licensing department from her work at SABC.

Celia completed her CGEIT, IT governance from ISACA, B. Com in Economics from the North-West University, and Master of Business Administration from Mancosa in 2013. She later completed her post-graduation and earned an MBA from the Gordon Institute of Business Science.
Lanx Goh
Global Head of Privacy for Prudential

Lanx Goh is the senior director and the global head of privacy at British multinational insurance company Prudential plc. He was the honorary consul of the Bulgaria Honorary Consulate in Singapore, where he worked towards improving bilateral ties between Bulgaria and Singapore to take their tourism, culture, education, and business to a new high.

Lanx joined the NUS Faculty of Law as a guest lecturer teaching data protection law to students and was later absorbed as the adjunct associate professor teaching protection and privacy laws and the practical aspects of data protection law. He worked at Singapore management university as a lecturer for over 4 years.

He was the head of international privacy at Ant Group, where he helped build an international legal team and global data protection office.

Besides being the data privacy and cybersecurity senior counsel at ByteDance and TikTok, Lanx was also the Global data protection officer and senior legal counsel of Klook. He served as the head of investigation at the prestigious personal data protection commission (PDPC) Singapore and was a devoted police officer at the Singapore Police Force for over five years.

He studied law at the University of Birmingham, graduated with a diploma in law from the National University of Singapore, and earned his Master of Law from the University of California, Berkeley. He further studied criminology and criminal justice by completing his Master of Science from the University of Oxford in 2014.
Chuck Brooks is the president of Brooks Consulting International and has won several awards, such as the Top 10 in Cybersecurity and Tech and the Top 2 Global Cybersecurity Expert and Influencer by Thinkers 360. He was among the top 50 Social Influencers in Risk and Compliance by Thompson Reuters and has been a two-time presidential appointee.

Brooks served on the advisory board of CISO Mag and was an esteemed member of the advisory panelist of MIT Technology. He was also a part of the Global advisory board of the EC-Council. He is a blogger, visiting editor for Homeland Security Today, and a featured contributor at GovCon.

Brooks has been an adjunct professor at Georgetown University for nearly five years now. While presiding over the president chair at Brooks Consulting International, he lent his expertise as a consultant for Fortune 1000 clients and has been a speaker for AT&T, Intel, and IBM. He has been a contributing writer at Forbes for over four years and has been a Gov Con expert, where he was recognized as a thought leader and a subject matter expert in cybersecurity and emerging technologies.

He was a part of the inner circle CISO advisory team at CyberTheory, contributing cyber panel expert at the Washington Post, an advisory board member at the WBAF Angel investment fund, and a strategic advisor at VIBE cybersecurity international LLC.

Brooks has many accolades to his name, including being a featured contributor at the High-Performance Counsel and a board member of several organizations, including the Franklin Foundation for Innovation. He also served as the vice president of government relations and marketing in Sutherland, as an advisor at the Bill and Melinda Gates Foundation, and was the director of legislative affairs at the Department of Homeland security between 2003 and 2007.
Chuck Brooks is The Cyber Express Cybersecurity Person of The Year 2022

“Cybersecurity is an imperative that encompasses people, processes, technologies, and especially shared knowledge. As connectivity and the sophistication of cyber-threats continue to multiply, cybersecurity will become a priority for industry and government to survive and thrive.”
We want to express our gratitude and congratulate each of you for being included on

*The Cybersecurity Person of the Year &
Top 10 Guardians of Cyberspace list.*

Your dedication to keeping our digital lives safe and secure is genuinely admirable, and we are honored to recognize your contributions to the field of cybersecurity.

We appreciate the crucial part you play in safeguarding the security of our systems and networks. You truly deserve all the recognitions, and we are grateful for your efforts.

Thank you for everything you do to make our world safer.
WEBINARS & EVENTS 2023
Connecting cyber professionals across the globe.
Saudi Arabia as Middle East’s Cybersecurity Hub: Challenges and Opportunities

Saudi Arabia’s Cybersecurity Systems Market size is projected to grow at a CAGR of 12.4% during 2020-2026 owing to a rapid increase in cyber-attacks and threats. What are the factors that go in Saudi’s favor? What are the challenges? Where do Saudi businesses stand in cybersecurity? Why should a cybersecurity business set up a shop in Saudi?

Participants: Vendors, Investors, Government officials, Industry professionals

Regions in focus: Cyprus, Israel, Lebanon, Palestine, Bahrain, Iraq, Jordan, Kuwait, Qatar, Saudi Arabia, Syria, Turkey, Yemen, Armenia, Azerbaijan, Georgia, Oman, UAE

Points to discuss:
1. Why is cybersecurity that important? Why should an individual, group or government care about cybersecurity?
2. Is cybersecurity a business decision or technical? Why should businesses worry about cybersecurity despite their size of operations?
3. Why are cross-border associations important in cybersecurity management?
4. How easy is it to open a cybersecurity business in Saudi Arabia? What are the special concessions that the sector receives from the government?
5. What about learning and development? Are Saudi universities capable of providing the manpower and training needed for the industry? (Optional)
6. UK offers priority visa clearance for medical and cybersecurity professionals. What is the Saudi policy on that?
7. What is the probability of Saudi becoming the cyber hub of the Middle East? What are the factors that you consider favourable?

Balancing Business and Security: The APAC Way

Security often comes at the cost of ease of business. Asian tech giants including Singapore, Thailand, and Philippines have had their way of updating and implementing cybersecurity laws without affecting the ease of doing business.

Key Takeaways:
1. How do nations manage to strike that balance?
2. How does the cybersecurity industry help the respective governments in achieving it?
3. Are businesses compromising ease for compliance or is it the other way around?
4. What about the geopolitical threats that run the risk of posing cyber threats to businesses?

Participants: Security companies, Advisories, Government officials, Industry professionals

Regions in focus: South East Asia, Eastern Asia, and South Asia
Graduates from top-ranked cybersecurity programs can expect to make six-figure starting salaries between $100,000 and $200,000, HR news services say. The US, particularly California, has a fine set of institutions that offer undergraduate and higher education programmes in various aspects of cybersecurity, often with significantly higher fees than their global peers. But is the current boom a stable trend or a bubble?

Participants: Vendors, Universities, Cybersecurity Placement consultants

Region in focus: USA

Key takeaways:
1. Entry-level qualification for cybersecurity has changed drastically
2. Industry and academia are working in tandem to meet the demands of the sector
3. Formal education: High entry barriers and role of industry support
4. Next big thing in technology education

Telcos in Switzerland are subject to stricter rules governing network outages and hacking incidents. ISPs there must detect and counter malicious activity – such as phishing attempts – on websites, blocking them if necessary. This poses questions on stealth browsing and the use of Tor or VPNs. How does Switzerland achieve better cyber monitoring with minimal invasion of privacy?

Participants: Telecom companies, Privacy advocates, Government officials

Region in focus: Europe

Key Takeaways:
1. How does Singapore manage that?
2. How does the cybersecurity industry help the government in achieving it?
3. Are businesses compromising ease for compliance or is it the other way around?
4. What about the geopolitical threats that run the risk of posing cyber threats to businesses?
Upcoming Events

World CyberCon Middle East Edition 2023
Riyadh, Saudi Arabia, 27 July 2023

World CyberCon APAC Edition 2023
Singapore, 24 November 2023

For more details please reach out to

<table>
<thead>
<tr>
<th>Mir Ali</th>
<th>Ashish Jaiswal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partnerships Manager</td>
<td>Conference Manager</td>
</tr>
<tr>
<td><a href="mailto:mir@thecyberexpress.com">mir@thecyberexpress.com</a></td>
<td><a href="mailto:ashish.j@thecyberexpress.com">ashish.j@thecyberexpress.com</a></td>
</tr>
<tr>
<td></td>
<td>+91 814 888 2990</td>
</tr>
</tbody>
</table>
Unlock **visibility** and **remediation** against adversaries and external threats with comprehensive cyber threat intelligence and digital risk protection.

Gain single pane of truth and end-to-end visibility across the external threat landscape through Dark web Monitoring, Cybercrime Monitoring, Attack Surface Exposure, Brand Monitoring, Threat Intelligence and Third Party (Supply chain) Risk Monitoring using its proprietary Cyble Vision platform.

Backed by AI-ML–powered predictive, personalized, and timely threat intelligence, Cyble processes billions of records on Deep, Dark, and Surface Web to offer near real-time coverage across adversaries, infrastructure, and targets.

www.cyble.com
<table>
<thead>
<tr>
<th>1</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Platform</td>
<td>Unique CTI Capabilities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent Filed</td>
<td>Threat Actors Monitored</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Detection and Alerting Capabilities</td>
<td>Threat Actors Monitored</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Operators Tracked</td>
<td>Global Sensor Networks Across Countries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML/Al Based Proprietary Risk Alerts</td>
<td>Near Real-time Visibility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Me</td>
<td>CYBLE VISION</td>
</tr>
</tbody>
</table>

Unlock visibility and remediation against adversaries and external threats with comprehensive cyber threat intelligence and digital risk protection.

Comprehensive Visibility into the unknowns of Dark Web and Cybercrime world

Gain single pane of truth and end-to-end visibility across the external threat landscape through Dark web Monitoring, Cybercrime Monitoring, Attack Surface Exposure, Brand Monitoring, Threat Intelligence and Third Party (Supply chain) Risk Monitoring using its proprietary Cyble Vision platform.

Backed by AI-ML-powered predictive, personalized, and timely threat intelligence, Cyble processes billions of records on Deep, Dark, and Surface Web to offer near real-time coverage across adversaries, infrastructure, and targets.

www.cyble.com

Digital Risk Protection through Actionable Threat Intel
Remediation through 3x Faster Takedown Support and Brand Monitoring

SCAN ME TO GET THE REPORT!
SCAN AND STAY UPDATED WITH REAL TIME CYBERSECURITY NEWS

To advertise with us, write to: marketing@thecyberexpress.com