MyConsultancy

NOVEMBER 2021

THE EVOLUTION OF CYBERSECURITY

IN THE DIGITAL AGE

MANOJ TAVARAJOO
DIVYA RAINJANA

The Evolution of Cybersecurity in the Digital Age

What is Cybersecurity?

In the recent month of October 2021, more than 600 journalists in 117 countries under the International Consortium of Investigative Journalists (ICIJ) exposed what is popularly known now as the Pandora Papers. The Pandora papers are a leak of nearly 12 million documents that report on hidden wealth, tax avoidance, and even money laundering by big, powerful names across the globe. These papers were gathered across 14 different sources in the span of several months and reveal how the rich and powerful—including some 330 politicians or more from 90 countries—utilise offshore tax havens to conceal their wealth from the world. According to the ICIJ, these identified offshore tax havens accumulate a hidden collective wealth of $5.6 trillion to $32 trillion in estimation. How did these investigative journalists orchestrate this leak? The most likely answer to that is due to the loopholes in cybersecurity.

Cybersecurity can be simply defined as the ability to protect or defend a cyberspace from cyber-attacks. What are cyber-attacks? Cyber-attacks are attacks that aim to disrupt, disable, destroy, or maliciously harm a computer environment or infrastructure. It can also destroy the integrity of the data and perform the action of stealing controlled information. Acknowledging this, the prominence of cybersecurity has significantly grown because information theft is the most expensive and valued kind of cybercrime. The pandemic has confined corporations and individual users alike to the limited level of cyber-safety they are accustomed to within their personal devices in their own homes—they are very likely to be more exposed to cybercrimes due to network vulnerability. Cybercrimes in 2021 have increased by 17% since last year, with the latest number of data compromise victims in the third quarter of the year soaring from 121 million to 160 million.

Cybersecurity is designed to protect two entities—the individual user and organisational bodies. Individual users include anyone with a personal smart device, and organisational bodies range from small companies to large corporations, including government bodies.

Forms of Cybersecurity Attacks

Cyber-attacks are simply a matter of when the hacking will occur. Most people feel that they are safe because they are not prominent figures or in possession of large wealth. Nonetheless, cybersecurity incidents have proven otherwise. The following are some of the most common forms of cyber-attacks that are usually deployed by cybercriminals.

Malware

Malwares are software programmes that are designed to inflict damage and unwanted actions on a computer. Examples of malware include viruses, trojan horses, worms, spyware, and ransomware. From a corporate perspective, these threats can cause a significant loss financially if they are not in possession of good cybersecurity measures to counter the attacks— especially

when it involves ransomware that demands financial compensation in exchange for the return of a debugged system.

Phishing

Phishing occurs when hackers send attacks to targeted users via email, asking them to click a link and enter personal details. If you are wondering how and why a user could fall for such a trick, it is because these emails and links are disguised and designed to look trustworthy and legitimate. These ‘dummy sites’ that the links lead to are programmed to then steal the personal data of the users.

Password attacks

Password attacks involve a third party trying to gain access into an account of a user by trying to guess the password. These guesses can be made by studying a user: From personal sentiments, online habits, and what they might use as their password based on their interests, hackers can use an algorithm to generate combinations of letters and numbers to try as passwords. Eventually, they hit the jackpot.

Denial of service attacks

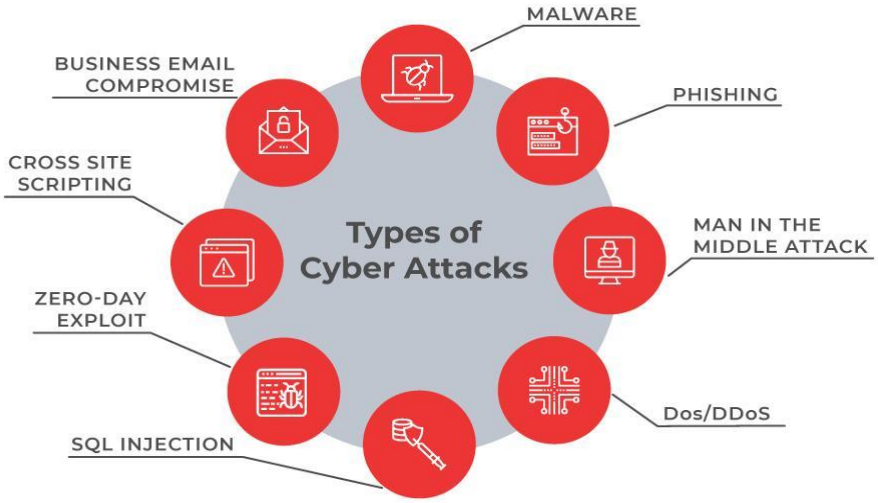
This cybersecurity attack occurs when hackers send high volumes of data and traffic to a site on the same network and server, causing them to be overloaded. This overload will cause the network and server to stop functioning, halting many online operations—especially companies and corporations.

Man In the Middle (MITM)

Man in The Middle, also commonly known as MITM, is when a hacker sits in between the user and the network in a place with a relatively less protected network status. These networks are usually public, such as those in cafes. Say a person is making an online transaction in a cafe, and then a hacker is trying to obtain information from that person, this hacker would just have to resemble the endpoints in the network in order to steal information from the user.

Drive-by downloads

A drive-by download is a kind of attack where the user goes to a website and a programme downloads automatically onto the laptop of the user. This download does not require any action to be done by the user, which makes it the most unsuspecting; unlike phishing where a user is led to click on a link voluntarily.



Source: Ecosystem Insights

Cybersecurity Trends to be Aware of in 2022

Minor forms of cyber-attacks can happen to anybody, but on an organisational and corporate level, it is important to be aware of new cybersecurity trends and the challenges they pose. Here is a brief look at the cybersecurity trends of 2022 that every organisation should adapt to in order to protect their data within the cyber-scape.

User Awareness

Awareness among users is important in order to identify and prevent network attacks by hackers to protect the consumer and the reputation of the organisation alike. Awareness campaigns should go beyond flyers and posters and into online programmes for organisations, curriculum for students (in both school and higher education), and in-house company training. These training sessions should include how to identify potential threats, how to protect basic data, and how to share confidential company data without being exposed to cyber-attacks.

Machine Learning (ML)

In 2022, the role of machine learning (ML) will make a wider expansion of use as it becomes intensely more proactive in the plane of cybersecurity. ML makes the job and operation of cybersecurity to be made more effective, simpler, and if not inexpensive, the process of it all certainly becomes less costly. ML develops and manipulates patterns with algorithms with the source of a rich dataset; through this, it is able to prepare and counter real-time cyber-attacks immediately. For ML to work at its optimum level, the dataset it relies on would have to be sophisticated and come from multiple points of view to produce effective algorithms. This varied and rich dataset analysed by ML will present as many scenarios as possible, allowing cybersecurity systems to learn and analyse patterns from cyber attackers. The outcome of this would be the prevention of future attacks and lesser routine checks by the cybersecurity department in an organisation.

Real Time Data Visibility

Presently, most company owners and organisational leaders do not have access to basic information about their own businesses. This basic information is truly a complete IT asset inventory—it includes a list of the hardware and software in use as well as third party suppliers. If companies do not have access to these kinds of information, what more can be said of not having access to analyses of potential cyber threats that have happened or may happen? This ought to change in 2022, as companies start being more vigilant and mindful of sensitive data in order to avoid all kinds of losses due to cybercrimes.

Cloud Security

As cloud services become increasingly adopted in organisational digital transformations, cloud security needs to be increased as well. Poor cloud security could easily lead to increased rates of cybercrimes, as it is not securely encrypted. The existence of innovative predictive security, however, plays a useful role in identifying attacks and threats posed by cybercriminals in order to fight against incoming data breaches.

IoT Vulnerability

As Internet of Things (IoT) devices become more rampantly in use, cybercriminals have identified more methods of hacking and breaching security measures, causing security problems to most IoT products today. IoT devices have computing devices installed into them to allow for the communication of data via the Internet, but this is also where cybercriminals expose these devices to hijacking attacks such as Dos. While IoT is set to expand its virtual products and services into our tangible society, home intrusions are expected to become a highly possible threat which will affect consumers and remotely conducted businesses alike.

Data Compromise in Higher Education

Similar to the predicament of the healthcare sector, organisations involved in the higher education sector are now focusing on increasing cybersecurity levels as well. Sending students, educators, and institutional staff into the realm of online learning has unfortunately opened doors for cybercriminals to steal student admissions data. To avoid more of these attacks, educational organisations are looking at innovative cybersecurity measures to protect not only student data, but also faculty and valuable research data within the institution.

Healthcare Sectors Become Targets

The healthcare sector is facing an increasing number of data violations and it is causing a huge financial loss on organisations within the field. This is because during the pandemic, restrictions of COVID-19 required healthcare organisations to loosen their firewall security to allow for staff to access information and work remotely. However, this is a gaping hole in which cybercriminals can use to steal confidential healthcare information. Healthcare organisations will up their security levels to meet the standard operating procedures of HIPAA (Health Insurance Portability and Accountability Act) in these challenging times while protecting important data.

Increasing Attacks on Financial Services

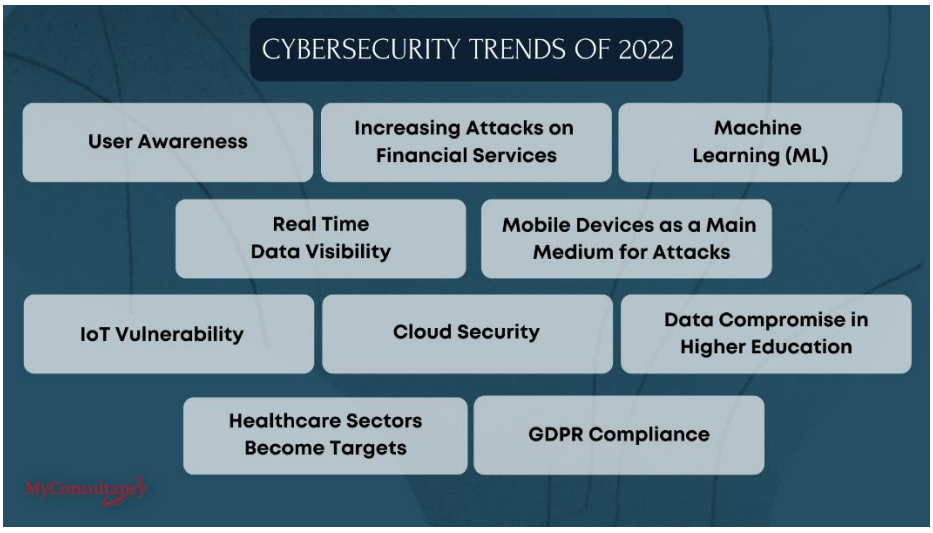
Another field exposed to cybercrimes is the field of financial services. Some financial institutions are still doing their best to be up to standard with current regulations and to incorporate cloud migration of data. In 2022, financial institutions may be prone to receiving more phishing attacks, malware attacks, as well as data breaches because unlike other industries—cyber-attacks can cause a large financial dent for a company. In 2020, The Washington Post reported a global corporate loss of $1 trillion due to cybercrime. This is because financial services are the most appealing targets to cybercriminals, as the amount of data is highly valuable. The permanent digital transformation of certain—if not most—companies (example: usage of cloud storage for data) allows them to leverage on multiple applications across multiple smart devices, but it also opens doors for cybercriminals to leverage instead on new ways to steal information.

Mobile Devices as a Medium for Attacks

Cybercriminals are using mobile smart devices as attack vectors because it is an easy way to steal information from vulnerable and unsuspecting users. The popularisation of mobile e-commerce software has enabled this method of cyber-attacks. It is an existing trend that will grow because everyone communicates for all purposes using a mobile device whether it is personal, business-related, for entertainment purposes, or even banking. That being said, an entire board of employees in a particular company could have personal and corporate information compromised in this method.

GDPR Compliance

Data privacy regulation experienced a significant development in nations across the European Union (EU) because of the General Data Protection Regulation (GDPR). The GDPR is currently imposing new and impactful regulations on companies that are marketing their services to residents in the EU nations in terms of stricter data protection requirements. A consistent and sustained security law on data is implemented on EU nations by the GDPR, removing the obligation of these nations to pen their own data security laws. Organisations involved with the EU's GDPR are steadily restructuring to comply with the changes; this ensures that consumer data of residents in the EU is protected.



Organisational Cybersecurity Strategies to Build Digital Trust

Cybersecurity is becoming more crucial each day. However, organisations may be overlooking its influence on customers and employees, who worry about their daily interactions with technology as attackers constantly look for new attack avenues. Building a cyber-security strategy that enables digital trust is the way forward. The following are recommendations on how organisations can build digital trust:

Re-envisioning the advancement of technology

It is important to consider two points of view in the field of cybersecurity, the first being a rising level of sophistication in a time of informational overload—this is considered to be a huge setback in the field of professional cybersecurity. The sophistication related to here will become more complex with the increasing interconnectivity of new digital endpoints. To make this easier for corporations, these complexities must be lessened to improve collaboration and automated responses to the cyber threats. This endeavour would also require the anticipation of new technology that poses a great level of potential in aiding the cybersecurity department of any company.

As for the second point of view, it is found by the observances done through a kind of security lens. The escalation of technology today disrupts existing business models, thrusting new methods of potential cyber-attacks upon them. In that sense, white hat hackers (ethical hackers in cybersecurity) should also leverage on the full potential of new technology as black hat hackers (cybercriminals) do. The digital tools chosen to incorporate into protecting the data of a company should cater to specific business requirements, threats, and risks—all of which require an in-depth understanding of the current needs of said company including the state of threat-filled cyber-scape that the company must deal with. Here are some recommendations for cybersecurity strategies on these two perspectives.

- ***Efficiency.*** Cybersecurity operations, services, and functions should be automated on an end-to-end basis, from the identification process to the recovery steps. While most of these services are done manually, the technology of automation with Artificial Intelligence (AI) can greatly improve the efficiency and quality of said services.
- ***Effectiveness.*** A risk-based approach is a wise manner to adopt when prioritising according to specific businesses. This would enable a cost-effective method as well, as money is spent in an area of a business's cybersecurity where it is needed and can provide productive results.
- ***Security.*** Security architects within the cybersecurity department should be tasked with building modern security architectures that make use of the latest technological advancements. In designing these modern security architectures, services should be resilient and follow principles that are based on verification instead of trust.

Expanding the digital accountability

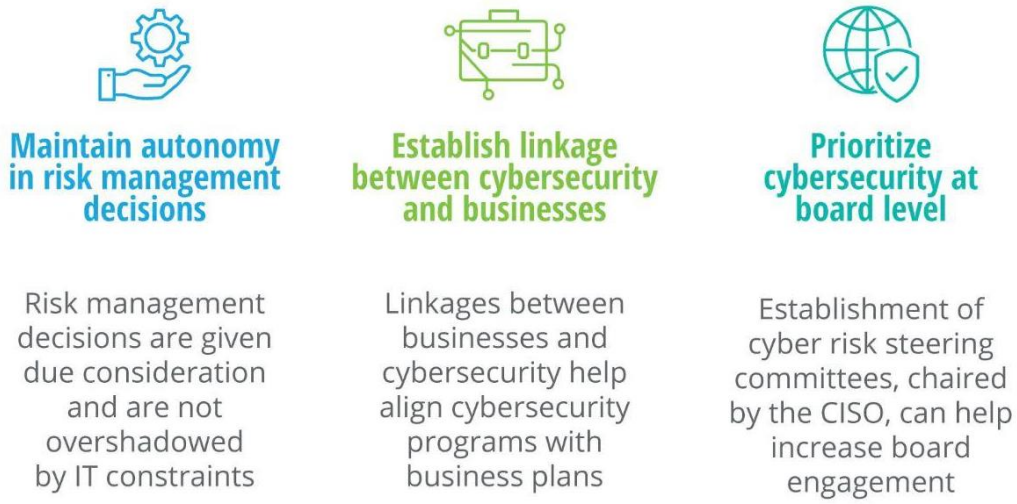
It is not an easy task for cybersecurity to create a digital environment that induces trust, the nature of this minefield of a cyber-scape has shifted from single stakeholders to multiple internal as well as external stakeholders. This means that the public pressure (including laws) has set the burden on various private and public-sector stakeholders that were not initially accountable for digital securities. The increasing sophistications mentioned previously demands that firms combine their internal entities in being responsible for cybersecurity. Governance models and responsibility needs to be reflected in the digital dimension, especially in terms of interconnectedness. Below are recommendations to ease this process for organisations.

- ***Co-creation approach.*** Modern cybersecurity strategies should be jointly developed with the entirety of the business including its system, from higher-ups to cybersecurity representatives.
- ***Shared responsibilities.*** Governance models within entire organisations should encompass clearly defined cybersecurity roles and responsibilities, including the technical and non-technical aspects alike. Responsibilities of cybersecurity components should also be divided and assigned accordingly amongst the stakeholders from the beginning of a process up to the post-production results.
- ***Prioritisation and customisation.*** The creation of strategy should meet the intended business objectives while maintaining the uncompromising protection of a company's important assets. This prioritisation will create a sense of trust, which is one of the primary reasons for cybersecurity.

Making the priority of data a ruling philosophy

The governance of data has expanded past regulation and privacy, as it is constantly diversifying. The relevance of data, however, should be recognised dynamically in cybersecurity strategies in corporations. As the technological plane switches to data and platform-driven digitised business models, personalised and smart services are more prominent. Instilling trust in these services is of primary concern because said services use personal information such as health statistics and details of financial transactions. That said, here are the recommendations in making data primacy a ruling philosophy.

- ***Redefinition of management in the life cycle of data***. This ever-interconnected world requires the rethinking of data life cycles to ensure useful application right from its creation to its deletion. This is critical because of the increasing number of devices and tools communicating with each other through interfaces.
- ***Framework creation.*** Technical and organisational measures should have specifically created frameworks to address increasing amounts of data. Developing cloud usage and cloud-provider capabilities should have their security standards consistently maintained and regulated. Open-source intelligence and security operations centres are examples of high-performance monitoring capabilities that should be established within corporations. Staying vigilant in this regard will allow real cyber threats to be identified more effectively.



Source: Deloitte, "How might cybersecurity retain independence within IT?"

Final Thoughts

The ever-changing landscape of cybersecurity serves as an important reminder to corporations across the globe that adapting to the current trends and advancements of technology is crucial in the protection of data. This fact should be a no-brainer, but as we have covered in this article, it is often overlooked especially in terms of cost and effectiveness.

Important highlights that companies should emphasise on regarding maintaining the security of their cyber realms include ensuring that their digitised measures are catered to their own business models. Sometimes, controlling the safety of a cyberspace from the perspective of the enemy is needed to ensure that all scenarios are thought of for automated responses to counter attacks. In accordance with that, it is vital that companies are up to date with the latest technologies in the field to implement into their cybersecurity measures to ensure that hackers do not get to them first. Companies suffer from five main damaging consequences when their data is breached, such as financial loss, reputational damage, operational downtime, legal action, and loss of sensitive data. In this digital age, building a cyber-security strategy that enables digital trust is the way forward.

ACCELERATING DIGITAL TRANSFORMATION.

www.myconsultancyonline.com

MyConsultancy