Infosys®
Navigate your next

VIEWPOINT

CYBERSECURITY: THE LONG VIEW

The history of cybersecurity can be seen as a series of increasingly complex and powerful waves — alternating between attacks and defenses. As the threats and costs of controls have increased, the role of chief information security officer has taken on greater importance in both the execution and the boardroom.

Infosys® | Knowledge Institute

Cybersecurity has grown in lockstep with the rest of technology, moving from a niche back office function to the top of the boardroom agenda. In less than a decade, the value of the global cybersecurity market has nearly tripled, with little slowdown in sight. It's expected to more than double by 2027 to $326.4 billion (Figure 1).

Even so, these ever-increasing investments have not been enough to stop — only temporarily slow down — the number and cost of attacks. A Forbes survey of chief information security officers (CISOs) found that lack of an adequate budget was among companies' top constraints in fighting cyberattacks.[1] Nearly all those CISOs predicted that attacks would increase, and one-fifth concluded that the abilities of cybercriminals outpaced the companies' defenses. It is not clear that organizations can spend their way to safety, however, this trend is changing. Organizations are now investing in cybersecurity as they see this as a strategic importance for their business.

Other challenges likewise hinder companies' ability to secure their systems, whether it is the increasing sophistication of the threats or the growing attack surface.

Cybersecurity has developed in stages: New threats emerge, those threats are solved, then even newer ones emerge. Each wave only gets more complex. At the same time, the number of security hacking incidents has continued to grow.

All the while, the importance of cybersecurity has steadily risen in the C-suite. What was once an information technology (IT) problem is now understood to be an existential threat that puts greater responsibility on the increasingly prominent CISO.

Taking the long view

To meet the challenges posed by the new wave of threats, leaders need to embrace different ways of thinking about and managing cybersecurity. Later in this paper, we recommend six actions companies should take to help protect themselves in this latest era of online danger.

First, that new approach requires context. Understanding the history of cybersecurity and the patterns that have developed over the decades can illuminate the path forward, and we've provided a brief overview below. A more in-depth history of cybersecurity and the signature developments and threats of each era appears at the end of this paper.

In the 1970s, computer viruses and worms were created as experiments without malicious intent. But with each new era, hackers' ambitions have grown and their methods for creating viruses and malware have been democratized —more people now have access to online weapons, and the damage they can inflict is far greater.

Infosys has divided cyberthreats into six eras to better understand their development and scope. We've just finished the Era of Expansion and have entered the Mainstream Era, where new digital tools and interconnectivity that fuel business development also open new avenues for threats.

Cybercriminals hacked software manufacturer SolarWinds and installed a malicious update in the Orion platform. Instead of hacking each organization separately, the supply chain attack took advantage of trusted software to create back doors to at least 18,000 clients worldwide. The breach went undetected for months and could have exposed data in the highest reaches of government, including the U.S. military and the White House.

Figure 1. The steep growth trend in the global cybersecurity market is projected to continue

Source: Infosys research

The chain reaction continued with the FireEye breach, which was also the result of the SolarWinds hack.[2] In December 2020, the Russian hacking group APT29, also known as Cozy Bear, stole a collection of cybersecurity firm FireEye's hacking tools.[3] While this was not the first incident where a cybersecurity firm was hacked, it served as a reminder that even those who are on top of their game can be compromised. And it further illustrated that our interconnected world is also a more vulnerable world.

Increasingly important role of the CISO

Among organizations worldwide, the CISO has been ascendant. These executives have to make some of their company's most difficult decisions, often with limited information. The role of these C-level executive leaders has evolved alongside the cyberthreats that keep them up at night.

By the mid-1990s, security was recognized as more than a technology issue. It was a business risk, which led to the creation of the CISO and the specialized cybersecurity office. Yet, in those early days, it was not a well-defined role.

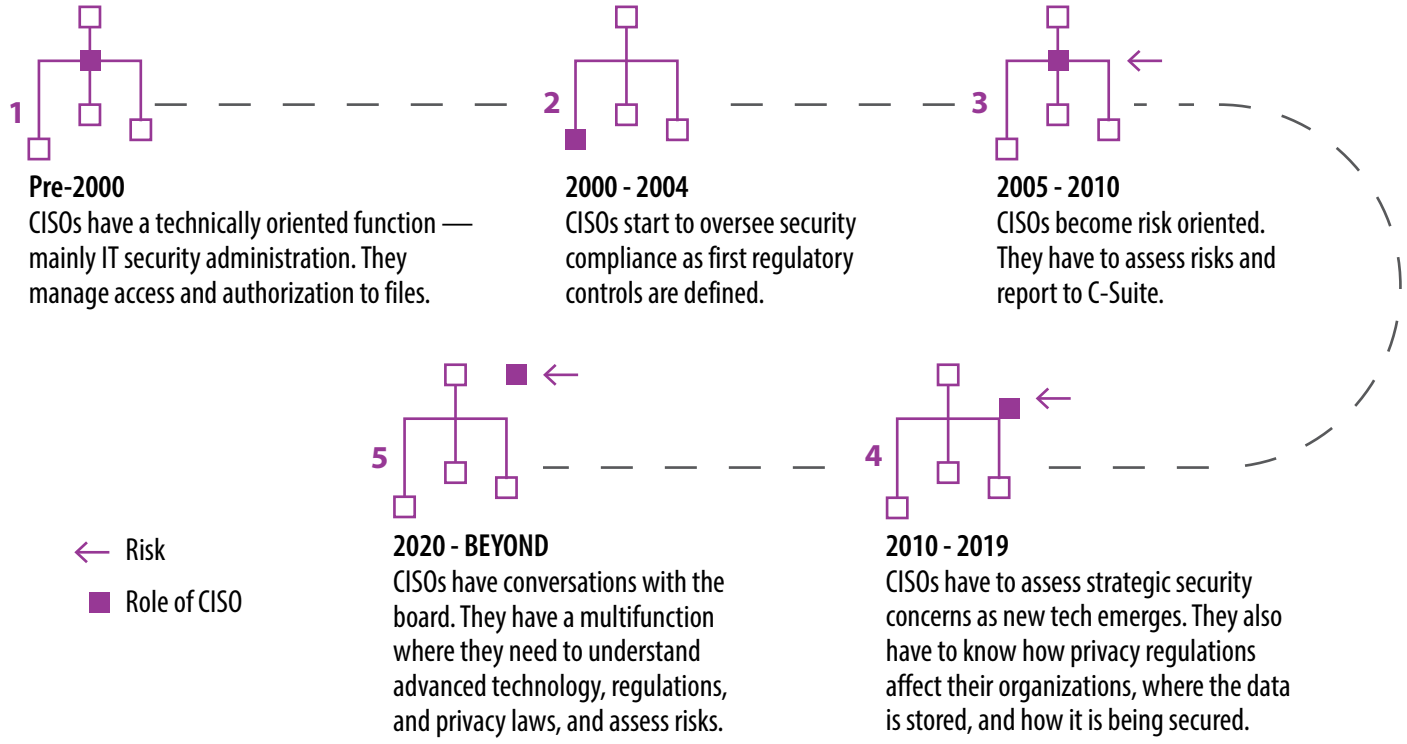
The job only started to transform into a management and leadership position in the 2000s. Cyberthreats became a major corporate problem, and the initial regulatory standards were introduced. So, CISOs not only had technically oriented functions but also oversaw security compliance.

By the mid-2000s, organizations became more attuned to risk. Nations developed their cyber capabilities and orchestrated espionage attacks on other nations. Geopolitical tensions added another function to the role of CISO. Starting then, CISOs had to assess big-picture risks and report to the rest of the C-suite.

Starting in 2010, the Era of Expansion saw the introduction of new technologies, such as the internet of things, migration to the cloud, and the exponential increase in social media. This led to the creation of new privacy and data regulations, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States. New technology and regulations added to CISOs' responsibilities. They not only had to assess strategic security concerns and unknown risks but also understand how privacy regulations affected their organizations, where their data was stored, and how it was secured.

In its short history, the CISO's role has evolved from mainly IT security administration to a complex C-level position. CISOs play an increasingly crucial role in organizations, and there are no signs that it will diminish. Today, these executives must understand advanced technology, regulations, and privacy laws; assess risks; and interact

Figure 2. Evolution of the CISO role



Source: Infosys research

with the board. Going forward, these executives will also have to better understand the cybersecurity risks of their companies' supply chains and partnerships. Rather than having responsibility for a single company, the CISO will bear the burden of securing an entire ecosystem.

The future of cybersecurity

Cybersecurity or privacy breaches are commonplace. Uncertainty and the lack of trust and collaboration within the cybersecurity ecosystem are getting in the way of an effective cyberdefense. The risks of cyberwar, absence of adequate regulations, and attribution difficulties exacerbate the problem.

The future of cybersecurity depends on the choices that companies, governments, and law-enforcement agencies make. If we continue repeating what we have already done, we will inevitably see progressively more and worse attacks — ones that are elements of daily operations rather than occasional threats. Cybersecurity tools created a couple of years ago, let alone defenses developed in past decades, are no longer good enough.

The SolarWinds hack is a wake-up call to the cybersecurity industry. Multiple networks will require a complete rebuild to isolate them from compromised networks. This is an opportunity for affected organizations to design new systems from scratch with security in mind.

> *"When the internet was born, nobody really worried about the security of the internet. That's how it was designed. And only when we started seeing the flaws being exploited did we start thinking about what we need to do."*
>
> ***Vishal Salvi**, Infosys' CISO and Head of the Cybersecurity Practice*

The same is true with networks and new solutions. To secure their future, companies need to build security into systems at the design stage, rather than chasing a patchwork solution for the latest threat. To reduce the number of future cyberattacks, organizations need to take six steps as quickly as possible.

Businesses need to gain a deeper understanding of the existing risks. We need more data on the threats, their nature, and the impacts of successful cyberattacks.

> Companies should introduce security into their networks and solutions during the design stage instead of relying on mere patches later

Companies should strengthen collaboration and information exchanges between private and public sectors on threat intelligence, incident reporting, and best practices for risk management and response.

Businesses are only as secure as their partners. Assess the risks of supply chain attacks and gain full visibility into third-party relationships. Organizations need to understand that every technological advance is also an open door to a new threat.

Companies and governments need to work toward better standardizing their regulatory approaches. Countries have different standards, laws, and regulations. They use different terminology related to cybercrime. Reducing these inconsistencies will facilitate greater communication and exchange of information, and improve apprehension and attribution problems.

Organizations must make security hygiene a foundational element of cybersecurity. Crisis preparedness and response protocols must be developed at both the national and international levels to enable organizations to respond and restore systems as quickly as possible.

Figure 3. Six steps to reduce cyberthreats

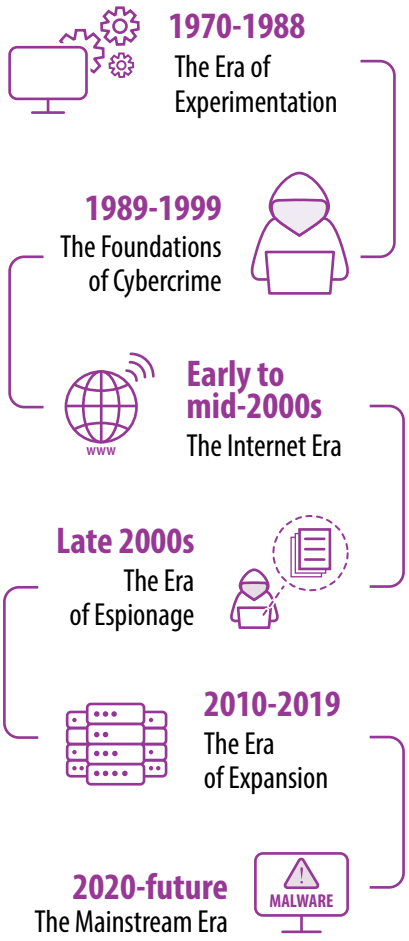
Source: Infosys

Last and most important, cybersecurity needs to be the topmost agenda item for companies that have any digital presence — which means every midsize or large business. In most cases, that will mean elevating the importance of the CISO.

With more money and more scrutiny, cybersecurity will continue to grow in importance — just as threats will grow in severity and often outpace defenses. The success of cybersecurity, however, will depend greatly on innovative strategies and different philosophies, rather than bigger budgets and newer tools.

The history of cybersecurity

To understand how we got to this point, we have analyzed major cybersecurity events over the past 50 years and divided them into six eras.



1. The Era of Experimentation (1970-1988)

The first viruses were developed in this era as innocent experiments. Initially, the programs were designed for research purposes and didn't have malicious intent. Still, the first self-replicating worm, first PC virus, and first virus that caused monetary damage were created during this period.

Major events

The 1970s marked the beginning of the viral era when Bob Thomas, a programmer at BBN Technologies, created **Creeper**. This was one of the first successful self-replicating programs that could spread over a network. The program did no harm; it only displayed the message "I`M THE CREEPER: CATCH ME IF YOU CAN."[4]

In response, Bob's colleague and the famous email creator Ray Tomlinson developed **Reaper**, a program designed to catch the virus. Reaper was the first step toward creating an antivirus program. However, the development of the first true antivirus programs happened two decades later.

In 1986, two Pakistani brothers created the first PC virus: **Brain**.[5] This infected 100,000 computers over three years. The brothers, owners of Brain Computer Services, wrote the virus to track pirated copies of their medical software. Brain consumed RAM, slowed hard drives, and sometimes interfered with saving data.

On November 2, 1988, a computer worm was distributed over the internet. The internet worm — better known as the **Morris worm** — was a major turning point in information security. Robert Morris, an American computer scientist, created the first computer worm on the internet as an experiment without malicious intent, but eventually, the computer program got out of control. It exploited vulnerabilities in thousands of computers, bringing their systems to a halt and causing an unknown amount of economic damage (estimated anywhere from $100,000 to $10 million).[6] It affected ordinary users as well as equipment operated by governments and military facilities. Although the worm didn't delete or damage files, it significantly slowed computing functions. The incident illustrated the vulnerability of computers and forced software vendors to take flaws in their products seriously. It also led to the creation of the Computer Emergency Response Team (CERT).[7]

2. The Foundations of Cybercrime (1989-1999)

The Morris worm exposed computer vulnerabilities and ended a more innocent period. In this next era, the foundations of cyber criminality were laid. Virus developers understood that their computer programs could be profitable. In 1993, the World Wide Web was publicly launched. Cybercriminals built their own websites as the number of internet users grew exponentially. In this period, crypto virology was born. The first macro virus and first social engineering attacks took place. Meanwhile, this era's innovation served as the basis for modern ransomware.

With the release of Microsoft Windows 98, software security went mainstream. The first anti-hacking products were introduced for home computers.

Major events

In 1989, Dr. Joseph Pop, evolutionary biologist and AIDS researcher, created the first money-extorting program: the **AIDS Trojan**. A user would receive a floppy disk by mail, which was supposed to contain information

about AIDS. Once the user installed the program, the ransomware would be activated. It eventually would hide all user files and block access, demanding a payment of $189.[8] Although the malware could be easily removed from the computer and the files could be decrypted, Pop's development opened a new world of human vulnerabilities. It also demonstrated that it is possible to profit from victims' ignorance and their dependence on computers.

In 1990, the **Computer Misuse Act** was passed in the United Kingdom and criminalized unauthorized access to computer systems. This was the first regulation that made cybercrime illegal.

The first antivirus software that could scan virus signatures was developed. In 1991, Symantec released **Norton Antivirus**. The same year, the **European Institute for Antivirus Research** was established to improve development of antivirus software.

In 1994, **Citibank** was hacked. Russian software engineer Vladimir Levin tricked the bank's system and transferred $10 million to accounts in different countries. Eventually, Levin was caught, and the bank recovered all the stolen money. This was the first cyber bank heist. As a result, the bank created a new C-level position, and Steve Katz became the first-ever CISO.[9]

Concept, the first macro virus, targeted Microsoft Word documents in 1995.[10] Macro viruses attacked data files by adding their code to the macros in documents and spreadsheets. After Concept, this type of virus became dominant until the turn of the 21st century. Their spread was mainly due to email's popularity as a way to exchange data. The ease of attaching files to a message and the ability of ordinary users to access the internet also contributed to the spread of macro viruses.

In 1996, hackers altered the U.S. Department of Justice and U.S. Air Force websites. That same year, the U.S. Department of Health & Human Services launched its **HIPAA** rule to protect the security and privacy of health information. Also, a crypto viral extortion protocol was invented that served as a foundation for modern ransomware.

The **Melissa virus**, the first macro virus with an email worm, was released in 1999. This was one of the first cyberattacks that used social engineering methods. Users received an email with an attachment (List.doc) that claimed to contain registration information for pornographic sites. As soon as the user opened the document, the virus accessed the victim's Microsoft Outlook program and forwarded the email to the first 50 contacts in the user's address book. Additionally, it infected every Word document stored on its victim's computer.

3. The Internet Era (early to mid-2000s)

By 2000, the internet had spread throughout the world, and hackers frequently targeted servers and public websites. Cybercriminals quickly learned how to exploit internet vulnerabilities and developed more damaging attacks. They could infect PCs, steal information, send spam, create phishing pages, and manage entire networks of computers to launch distributed denial of service (DDoS) attacks. Computer worms spread exponentially; there were more than 1 million of them by the mid-2000s.[11]

The increase in attacks made companies reconsider their security priorities and recognize cyberthreats as a major corporate problem. In 2004, the global cybersecurity market was worth $3.5 billion. The cybersecurity industry responded to threats with antivirus software, firewalls, and VPN solutions. In the early 2000s, regulatory standards like BS-7799/ISO 27001 were developed.[12]

Major events

In 2000, the **ILOVEYOU worm** infected millions of computers worldwide within a few hours of its release. Inspired by the Melissa worm, ILOVEYOU used more aggressive social engineering strategies. Disguised as a love letter, the virus was sent in an email. Once victims opened an attached file, the Trojan would automatically install onto their computers. It then would overwrite files, steal users' data, lock the users out of their email accounts, and forward itself to everyone on the victims' contact list. ILOVEYOU is regarded as one of the most damaging worms and was responsible for an estimated $10 billion in damage.[13]

In 2000, a 15-year-old Canadian hacker launched an attack against several e-commerce websites, including Amazon and eBay.[14] This was the first documented **DDoS** attack.

Microsoft published a book on secure code development, **Writing Secure Code**, in 2001. The book was an official acknowledgment of how important the software giant considered security. From this moment, it was clear that simply writing the code and selling the product was not enough — ensuring security was equally important.

In 2003, the **SQL Slammer worm** caused a denial of service on internet hosts. The worm infected more than 75,000 machines within 10 minutes. Also, the decentralized "hacktivist" group **Anonymous** formed in that same year.

As fraud increased, an industry consortium — featuring American Express, Discover Financial Services, JCB International, MasterCard, and Visa — released its **Credit Card Security Standard** in 2004. This created baseline security controls on all aspects of handling credit card information.

4. The Era of Espionage (late 2000s)

Cyberthreats became political in the mid-2000s. Nations realized that digital attacks could be used for spying and to cause physical disruption. Cybercriminals targeted cities, states, and critical infrastructure. This affected national security and cost businesses millions of dollars. During this era, the first state-sponsored cyber gangs formed. It also became evident that any country with a sufficiently well-developed network infrastructure was vulnerable to cyberthreats.

Major events

In 2007, **Russian-backed hackers** launched DDoS attacks on websites of Estonian companies, including the country's Parliament, banks, ministries, newspapers, and broadcasters. Also, the **Storm** botnet was created from hacked computers.

APT10, an espionage group backed by the Chinese government, stole information from various countries in 2009 to meet Chinese national security goals. That same year, the **HITECH Act** in the United States became law. This regulation aimed to ensure the security and privacy of health information.

In 2010, the first malware conference, **MalCon**, took place in India with support from the government. Also, the Israeli-American **Stuxnet** malware, which is considered to be the first cyber weapon, attacked Iran's nuclear facilities in 2010.[15] The malware damaged several uranium centrifuges and eventually infected more than 200,000 computers. Stuxnet exploited a Windows zero-day vulnerability.

5. The Era of Expansion (2010-2019)

In the Era of Expansion, or era of major breaches, attacks became even more expensive and proved they could damage physical infrastructure. A cyberattack could devastate a company's reputation in moments, resulting in loss of business and even bankruptcy. During this era, hackers frequently launched zero-day attacks, compromised smart devices, and used aggressive social engineering tactics. They also interfered with political elections and altered public opinion via the spread of fake news.

The value of the global cybersecurity market was $64 billion in 2011.[16] By the end of this era, it had more than doubled to an estimated $156.45 billion.[17]

To counter the growing number and scope of attacks, cybersecurity professionals developed new technologies: application-aware firewalls, threat management, threat hunting, threat intelligence analytics, deep packet inspection, malware analysis, big data analytics, DevSecOps, and others. During this period, the National Institute of Standards and Technology (NIST) framework and Information Security Forum (ISF) standards of good practices were introduced. In 2019, zero-trust frameworks, blockchain technology, container security, breach attack simulation, and NDR/CDR solutions gained prominence.[18]

Major events

In 2011, **RSA**, a security firm that sells the SecureID authentication system, was breached. Hackers sent phishing emails to employees with a zero-day attack that exploited an Adobe Flash vulnerability. Eventually, the attackers gained access to SecureID authentication parameters. The breach cost parent company EMC $66.3 million.[19]

In 2012, **Operation Ababil**, a series of DDoS attacks, was launched against U.S. financial institutions. The New York Stock Exchange, Bank of America, JPMorgan Chase, SunTrust Bank, and others were affected. The attacks were determined to be Iran's retaliatory campaign against the United States.[20]

Hackers gained access to 3 billion **Yahoo accounts** in 2014. The Yahoo attack is the largest reported data breach to date. The company didn't report the breach until 2016.

In 2016, the first wave of IoT device hacks started. The **Mirai botnet** was created from a large number of cameras and routers by selecting combinations of default usernames and passwords. The network was later used for a powerful DDoS attack. From 2016 to 2017, the number of attacks on IoT devices increased by 600%.[21]

The **GDPR** was created in 2018 and became the primary law that regulates how corporations protect EU citizens' personal data. The regulation requires businesses to report a breach within the first 72 hours of its occurrence.

> The Yahoo attack in 2014 has been the biggest data breach to date, affecting over 3 billion accounts

In 2016, **WikiLeaks** published documents from the 2016 Democratic National Committee email leak. The leak happened during the U.S. presidential election, and the material was used against candidate Hillary Clinton and her party.

APT10 launched **Operation Cloud Hopper** in 2016.[22] The campaign attacked cloud service and managed IT service providers. Hackers stole intellectual property and other sensitive data.

In 2017, credit-reporting agency **Equifax** was breached. Attackers stole the personal data of 143 million American, Canadian, and British consumers as well as 200,000 credit card numbers.[23] The data included

names, dates of birth, addresses, bank account numbers, Social Security numbers, and driver's license numbers.

In 2017, the Shadow Brokers hacker group leaked **EternalBlue**, a critical exploit developed by the U.S. National Security Agency. The exploit was in turn used in the WannaCry and NotPetya attacks.

That same year, **WannaCry** ransomware infected more than 230,000 computers in more than 150 countries in a single day.[24] It used a Windows zero-day exploit to spread. When the ransomware infected computers, it demanded a payment in cryptocurrency to decrypt files. But even if a victim paid the ransom, the files were not decrypted. The WannaCry damage is estimated at between $4 billion and $8 billion.[25] Many companies were affected in addition to the United Kingdom's National Health Service. Microsoft released a patch for EternalBlue — the underlying flaw — and computers that updated their software are no longer vulnerable to WannaCry.

Also in 2017, another major ransomware attack — using the same vulnerability — shook the world. Even though it took advantage of an already patched exploit, **NotPetya** infected thousands of computers because many of them didn't install updates. Unlike WannaCry, NotPetya was a targeted attack. It is believed that it was originally aimed at Ukraine but spread across the world. Many large companies suffered from the attack, including Maersk, FedEx, and Merck & Co. The global cost of the NotPetya attack was estimated at $10 billion.[26]

In 2018, the **Marriott data breach** became public. Starwood Hotels confirmed that as many as 500 million hotel guests' information, including bank data, was stolen.[27] The data breach had started at least by 2014.

The same year, **Facebook** confirmed that the data of 50 million users was at risk after attackers exploited a vulnerability that allowed them to take over accounts.[28]

In 2018, the **CCPA** launched. The statewide data privacy law gives consumers in California more control over which personal data businesses worldwide can collect.

Norsk Hydro, the Norwegian aluminum giant, was hit by the **Lockergoga ransomware** in 2019. The company refused to pay the ransom but was able to restore its operations from backup servers. Although the company didn't pay a single bitcoin, the cost of the breach still amounted to $71 million.[29]

6. The Mainstream Era (2020-future)

Because of today's interconnectivity and digital partnerships, malicious actors can use the vulnerabilities of a company's partner to collect information in stealth mode. So even when criminals create a malware that is not intended for your organization, you can still be a victim.

Current cybersecurity solutions focus their defenses on workspace transformation, cloud adoption, digital transformation, and borderless architecture.

Major events

Chinese hackers targeted over 75 organizations around the world in manufacturing, media, health care, and nonprofit sectors as part of a wide-ranging cyber espionage campaign.

North Korean state hackers sent COVID-19-themed phishing emails to more than 5 million businesses and individuals in Singapore, Japan, the United States, South Korea, India, and the UK in an attempt to steal personal and financial data.

In December 2020, cybersecurity firm **FireEye** became a victim of a state-sponsored attack. The attackers identified vulnerabilities in the **SolarWinds**' cybersecurity architecture and installed the malware-ridden update on 18,000 computers of SolarWinds' customers.

> New cybersecurity solutions rely on a combination of cloud adoption, digital transformation, borderless architecture, and workplace transformation

It's impossible to know the full scope of this era, which has barely started. But if trends continue, it will be shorter than the last but no less transformative. As risks become intertwined among partners and throughout supply chains, the threats will keep cybersecurity at the top of the agenda and embedded even deeper into the enterprise.

References

1. Forbes CISO Research: Managing Risks with Limited Resources, Aug. 20, 2019, Security Boulevard.
2. SolarWinds Hack Could Affect 18K Customers, Brian Krebs, Dec. 15, 2020, Krebs on Security.
3. FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State, David E. Sanger and Nicole Perlroth, Dec. 8, 2020, The New York Times.
4. The First Computer Virus of Bob Thomas (Complete History), Georgi Dalakov, History Computer.
5. How Two Pakistani Brothers Created the First PC Virus, Jason Kersten, Nov. 2, 2013, Mental Floss.
6. Flashback Tuesday: The Morris Worm, Nov. 2, 2016, WeLiveSecurity Magazine.
7. The Morris Worm: 30 Years Since First Major Attack on the Internet, Nov. 2, 2018, U.S. Federal Bureau of Investigation.
8. A Brief History of Computer Viruses, AVG Signal Blog.
9. Backstory Of The World's First Chief Information Security Officer, Steve Morgan, Oct. 13, 2020, Cybercrime Magazine.
10. What is Macro Virus? – Definition, Kaspersky.
11. The Evolution Of Malware, Fred Touchette, Oct. 2, 2015, Dark Reading.
12. Cyber Security – Safeguarding Your Digital Journey, Ramesh N., 2020, Infosys Knowledge Institute.
13. A Brief History of Computer Viruses, AVG Signal Blog.
14. Denial of service attack, Britannica.
15. What is Stuxnet, who created it and how does it work?, Josh Fruhlinger, Aug. 22, 2017, CSO.
16. Want job security? Try online security, Alec Ross, April 25, 2016, Wired.
17. Cyber Security Market Size, Share & Trends Analysis Report 2020-2027, June 2020, Grand View Research.
18. Infosys Tech Compass, Infosys Knowledge Institute.
19. RSA Breach Costs Parent EMC $66.3 Million, Eric Chabrow, Aug. 1, 2011, Data Beach Today.
20. Iran Crisis Moves Into Cyberspace, Micah Loudermilk, July 9, 2019, The Washington Institute for Near East Policy.
21. As IoT attacks increase 600% in one year, businesses need to up their security, Alison DeNisco Rayome, March 21, 2018, TechRepublic.
22. Operation Cloud Hopper, April 2017, PwC.
23. Equifax data breach FAQ: What happened, who was affected, what was the impact?, Josh Fruhlinger, Feb. 12, 2020, CSO.
24. WannaCry: Lessons Learned 1 Year Later, Charles Cooper, May 15, 2018, Symantec.
25. Is the world ready for the next big ransomware attack?, Dan Swinhoe, March 4, 2019, CSO.
26. The Untold Story of NotPetya, Andy Greenberg, Aug. 22, 2018, Wired.
27. Marriott data breach FAQ: How did it happen and what was the impact?, Josh Fruhlinger, Feb. 12, 2020, CSO.
28. Everything We Know About Facebook's Massive Security Breach, Louise Matsakis and Issie Lapowsky, Sept. 28, 2018, Wired.
29. Hackers hit Norsk Hydro with ransomware. The company responded with transparency, Bill Briggs, Dec. 16, 2019, Microsoft.

Subject Matter Expert

Vishal Salvi

SVP, CISO, head of Cybersecurity Practice, Infosys
vishal.salvi@infosys.com

Author

Yulia De Bari

Consultant, Infosys Knowledge Institute
yulia.debari@infosys.com

Producer

Jeff Mosier

Editor-at-large, Infosys Knowledge Institute
jeff.mosier@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next