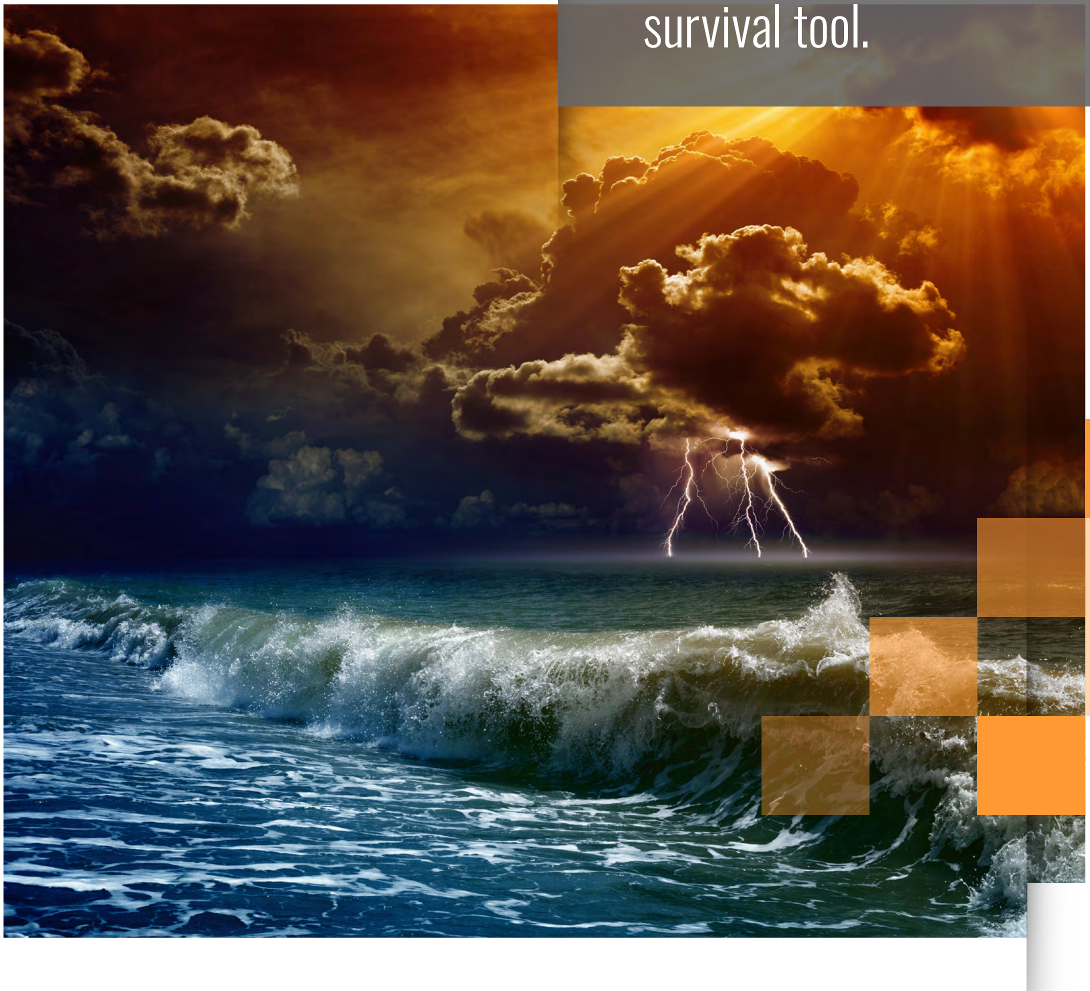
KnowBe4
Human error. Conquered.

Can The Public Sector Face The Coming Wave Of Attacks?

> Enabling the human firewall is becoming an increasingly essential survival tool.



Citizens cannot opt out of giving government agencies or public institutions their most personal and private information, whether their financial details, their diseases and medications, or their children's health and education records. When this personal data ends up on the dark web at the hands of an anonymous hacker, it is personally devastating; it also opens the victims up to harassment, identify theft, and fraud, and shatters their trust in the agencies they need to trust most.

Given the level of damage that can be caused by these attacks, it should not be surprising that the public sector is becoming an increasingly attractive target for cybercriminals. But just how attractive is alarming.

According to Blackberry's second Quarterly Threat Intelligence Report in August 2023,[1] cyber-attacks against government agencies and public sector services were up 40% in the second quarter of 2023 compared to the first. Government and public entities were among the top four attack targets.

Dmitry Bestuzhev, senior director of BlackBerry's Threat Research and Intelligence team, called government data on its citizens "gold", saying that "getting their hands on this sensitive data is considered 'absolute success' for both nation-states and financially motivated threat actors. It can also be used in additional cyber-attacks, such as high-quality spear phishing attacks."[2]

The value of the personal information held by the public sector is compounded, in the eyes of a threat actor, by the ease of access. Publicly funded organizations often have immature cyber defense programs and limited resources, leaving them struggling to defend themselves against increasingly sophisticated attacks.

[1] https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report

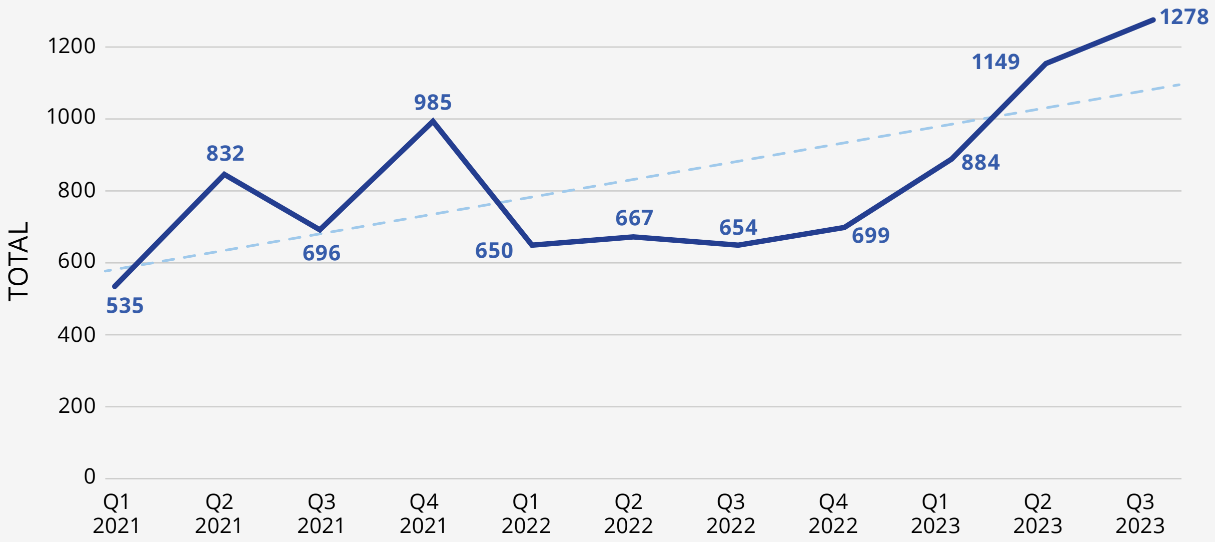
[2] https://www.infosecurity-magazine.com/news/cyberattacks-government-agencies/

ACROSS SECTORS, CYBER ATTACKS ARE SOARING

From all perspectives, global cyber attacks have continued a meteoric rise in 2023. In the third quarter of the year, global ransomware attacks were up 95% over 2022.[3] The global average cost of a data breach jumped to $4.45 million this year, a 15% increase in the last three years.[4] According to FBI and IMF data, the global average annual cost of cybercrime is expected to soar from $8.4 trillion in 2022 to more than $23 trillion in 2027.[5]

Corvus Insurance, the leading cyber underwriter, analyzes data from ransomware leak sites (websites on the dark web where ransomware groups post stolen data) to track evolving trends. In October 2023, the company released its Q3 findings, which showed ransomware attacks continued at a record-breaking pace; Q3 global ransomware attack frequency was up 11% over Q2 and 95% year-over-year.[6]

RANSOMWARE LEAKS OVER TIME, BY QUARTER CORVUS INSURANCE



According to the report, government agencies and law practices were the two sectors showing the largest spike in ransomware in Q3 of 2023, with a 95% increase in ransomware attacks. LockBit, a commonly used form of ransomware, tripled their government victims from Q2 - Q3, primarily attacking cities or municipalities.[7]

Social engineering and its multiple variants -- phishing, vishing, spear phishing, smishing, and others -- remain the most common entry point for between 70 and 90% of all malicious breaches.[8] Business Email Compromise (BEC) remains another favorite, while Pretexting, a sub-category that includes the use of a fabricated story to gain a victim's trust, has nearly doubled over 2022.[9]

But we may just be getting started. AI- and generative AI-enabled attacks promise to transform the entire cyber threat landscape, as hackers adopt AI more rapidly, and in some cases with more sophistication, than enterprise technology teams.[10]

[3] https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report
[4] https://www.ibm.com/reports/data-breach
[5] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
[6] https://www.corvusinsurance.com/blog/q3-ransomware-report
[7] https://www.corvusinsurance.com/blog/q3-ransomware-report
[8] https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks
[9] https://www.verizon.com/business/resources/reports/dbir/
[10] https://www.csoonline.com/article/651125/emerging-cyber-threats-in-2023-from-ai-to-quantum-to-data-poisoning.html

Aside from using Generative AI (GenAI) to develop new malware, AI tools allow threat actors to better engineer the actions of vulnerable employees, including creating messages and even phone calls that more accurately mimic the natural language and design of trustworthy colleagues and partners. It allows them to heighten the speed, scale, and scope of their attacks, and to analyze attack strategies more accurately for improved success rates.

One of the reasons for the increasing capacity of threat actors and their swift adoption of new technologies is the evolution of their organizational structure. If you still think of hackers the way they are portrayed in stock photo or crime shows, as three or four young people wearing hoods and hunkered down behind their laptops, those days are gone. As noted in Fortinet's Global Threat Landscape Report,[11] in 2023, many cybercrime organization and nation-state cyber offensive groups "operate much like traditional enterprises, complete with well-defined responsibilities, deliverables, and objectives. This organizational structure, combined with deep pockets resulting from past exploits or nation-state sponsors, facilitates their offensive stance, allowing them to experiment with and incorporate game-changing technologies, such as new generative AI, that make their attacks more complex and harder to detect ."

So in five years we may be looking at the 2023 cyber attack statistics and saying, "Remember when we thought that was a lot?"

This did not need to be a surprise. In 2019, Forrester Research reported[12] that 80% of cybersecurity decision-makers expected AI to increase the scale and speed of attacks and 66% expected AI "to conduct attacks that no human could conceive of." The report said that "these attacks will be stealthy and unpredictable in a way that enables them to evade traditional security approaches that rely on rules and signatures and only reference historical attacks."

In other words, the human has long been the most vulnerable point of a network – the easy mark for cybercriminals. With AI, humans have become both more vulnerable and easier to deceive. And the hackers are getting better at using it than we are.

Fortunately, this does not need to be a doomsday scenario. The strongest tools against the onslaught are not complex or out of reach. Strengthening the human factor, the most vulnerable point in the entire threat landscape, continues to be the simplest and most cost-effective tool against social engineering in all forms. But as the attacks on the human element become more "intelligent," enabling the human firewall is becoming an increasingly essential survival tool.

[11] https://www.fortinet.com/resources-campaign/cybersecurity-platform/report-global-threat-landscape-1h-2023

[12] https://www.snowdropsolution.com/pdf/The%20Emergence%20Of%20Offensive%20AI.pdf

NORTH AMERICA

UNITED STATES

On first inspection, there is good news for companies when it comes to surveyed workers' attitudes towards cybersecurity.

A high percentage of hybrid (86%) and remote (86%) workers surveyed say that they feel responsible towards their company's cybersecurity, this then drops slightly for those who work full-time in the office, where just under 4 in 5 (79%) feel responsible towards their company's cybersecurity. In fact, just over a fifth (21%) of full-time office workers do not feel responsible towards their company's cybersecurity, compared to 1 in 7 remote or hybrid workers (both 14%). This is perhaps good news for businesses given that remote and hybrid ways of working tend to present more of a cybersecurity challenge.

Overall, the findings indicate that a significant proportion of workers do feel responsible for their company's cybersecurity. However, further analysis of the data reveals that this is not always supported by secure behaviour.

An attack on the 36,000-student Minneapolis Public Schools in March 2023, illustrates the level of devastation and loss of trust brought about by cyber attacks on the public sector. A ransomware attack by the Medusa group exfiltrated a trove of data including personal information on students; the attackers demanded a $1 million ransom to keep the files from being leaked. The files were leaked.

The stolen documents included descriptions of sexual assault, psychiatric hospitalization, parental abuse, truancy, and suicide attempts[13]– information given by parents and students who trusted their officials that the data would remain private. Other exposed records included medical records, discrimination complaints, Social Security numbers and contact information of district employees.

In February, the city of Oakland, California, was targeted by ransomware group Play in an attack that brought down nearly all of the systems the city uses to serve its nearly 500,000 residents. The group then leaked 10GB of city data, including, according to the group, "private and personal confidential data, financial, gov, etc. IDs, passports, employee full info, human rights violation information."[14] This was followed by another 600GB of city data in March, including "troves of documents" stolen from the city police department.

Also in February, the U.S. Marshals Service suffered an attack[15] on a computer system that held sensitive law enforcement data belonging to the Technical Operations Group (TOG) that provide surveillance capabilities to track fugitives. Critical tools were out of operation for 30 days. Stolen data included employees' personally identifiable information alongside returns from legal processes, administrative information and PII pertaining to subjects of USMS investigations and third parties.In May 2023, a prominent Texas city was forced to shut down a number of its IT systems, including police and fire department services, in an attack that exposed names, addresses, and medical information of more than 26,000 people including city employees. Some city employees have already reported identity theft; some of their children have had personal information stolen as a result of the identity theft. In August, their City Council approved $8.6 million in payments for services relating to the attack.[16]

These are only examples. And they do not let up as the year goes on. In September, a community college in Ohio notified 290,000 people of a data theft breach[17] that had happened in Spring that

[13] https://apnews.com/article/schools-ransomware-data-breach-40ebeda010158f04a1ef14607bfed9b0
[14] https://therecord.media/oakland-officials-say-ransomware-group-may-release-personal-data-on-saturday
[15] https://edition.cnn.com/2023/05/01/politics/us-marshals-ransomware-attack-fugitives/index.html
[16] https://www.govtech.com/security/dallas-approves-8-6m-in-ransomware-response-payments
[17] https://www.bankinfosecurity.com/ohio-community-college-data-theft-breach-affects-nearly-300k-a-23132

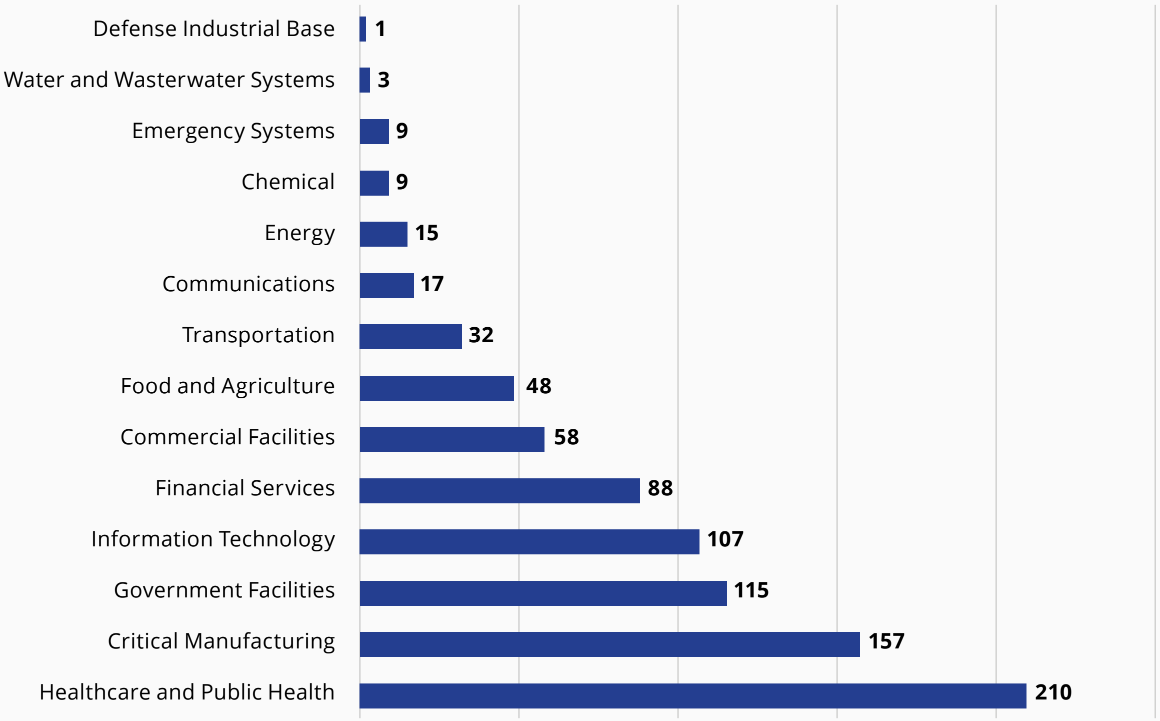
may have compromised their personal, financial and health information. Information impacted is said to include individuals' names, Social Security numbers, driver's license numbers, financial account information, credit or debit card information, passport numbers, medical information, and health insurance policy information. The same month, a community school district in Indiana confirmed that it had been a victim of a ransomware attack in the previous year. The attack occurred when a staff member fell for a phishing email which resulted in the encryption of files on the school district's servers. The district Superintendent said that the ransom was paid, and student and staff information was given back to the school district. But in total, the ransom payment, technology updates and payments to specialists and legal teams cost the school district $1million.[18]

Also in September, The Snatch ransomware crew listed a Florida government agency on its dark-web site as one of its latest victims.[19] Per reports, negotiations were ongoing between the agency and the hackers, but the talks may have broken down. No one is talking much.

In October, the District of Columbia Board of Elections disclosed that 600,000 lines of voter records have been compromised in an attack by the RansomedVC ransomware operation against the Board's website hosting provider.[20] Exfiltrated data, including voters' addresses and driver's license numbers, as well as the last four digits of their Social Security numbers, has already been offered for sale on a hacking forum. The attack came just months after the breach of DC Health Link, the city's health insurance exchange, that exposed the data of senior national security officials.[21]

In the category of critical infrastructure, in March 2023, IC3 (the FBI's Internet Crime Complaint Center) reported that public sector agencies and institutions dominated the categories of targets for cyber attacks in the U.S. Healthcare and public health was the critical infrastructure sector most targeted by ransomware, followed by critical manufacturing and government facilities:

INFRASTRUCTURE SECTORS VICTIMIZED BY RANSOMWARE



[18] https://www.govtech.com/education/k-12/crown-point-community-schools-confirms-ransomware-attack
[19] https://thecyberexpress.com/snatch-ransomware-group-fdva-cyber-attack/
[20] https://www.scmagazine.com/brief/data-breach-exposes-dc-voter-data
[21] https://www.scmagazine.com/news/dc-health-link-says-human-error-led-to-congress-members-stolen-data

We should be bracing ourselves for even more in the 2023 reports. According to experts speaking at Tech Crunch's Disrupt Conference in September 2023 is on track to shatter the records for ransomware attacks targeting public sector institutions and industries in the United States.

MK Palmore, former FBI agent and director in Google Cloud's Office of the CISO, said that while public sector organizations are rapidly expanding their digital footprints, many are adding a huge amount of complexity to their environments that often only a small number of security practitioners are responsible for protecting.

"That challenge," he said onstage, "can be relatively insurmountable."

CANADA

PwC's Canadian Cyber Threat Intelligence Report,[23] issued in August 2023, notes that Canada's threat landscape has also shifted radically in the last year, fueled by "mounting geopolitical tensions, fluctuating economic conditions and rapid digitization in the wake of the pandemic."

Like the U.S., the report notes that "As governments and businesses grapple with how to enhance their resilience in the face of the evolving risk environment, threat actors are embracing artificial intelligence (AI) and other innovations to enhance their attack strategies and power a broader array of increasingly complex and sophisticated cyber attacks."

The report highlights the top cyber threats in the past year, which include sophisticated attacks such as ransomware, state-sponsored threat actors, supply chain disruptions, phishing attempts, and exploitation of vulnerabilities and gaps in cloud computing.

In November 2023, the Canadian government issued a statement saying that two of its contractors, both related to relocation services, had been hacked in October, exposing sensitive information belonging to an undisclosed number of government employees. Both companies provided relocation services to Canadian government employees.

According to the statement,[24] the breached information could go back 24 years. It "could belong to anyone who has used relocation services as early as 1999 and may include any personal and financial information that employees provided to the companies." The victims include a broad spectrum of affected individuals, including members of the Royal Canadian Mounted Police (RCMP), Canadian Armed Forces personnel, and Government of Canada employees. LockBit ransomware gang has claimed responsibility for breaching SIRVA's systems and leaked what they claim to be archives containing 1.5TB of stolen documents.

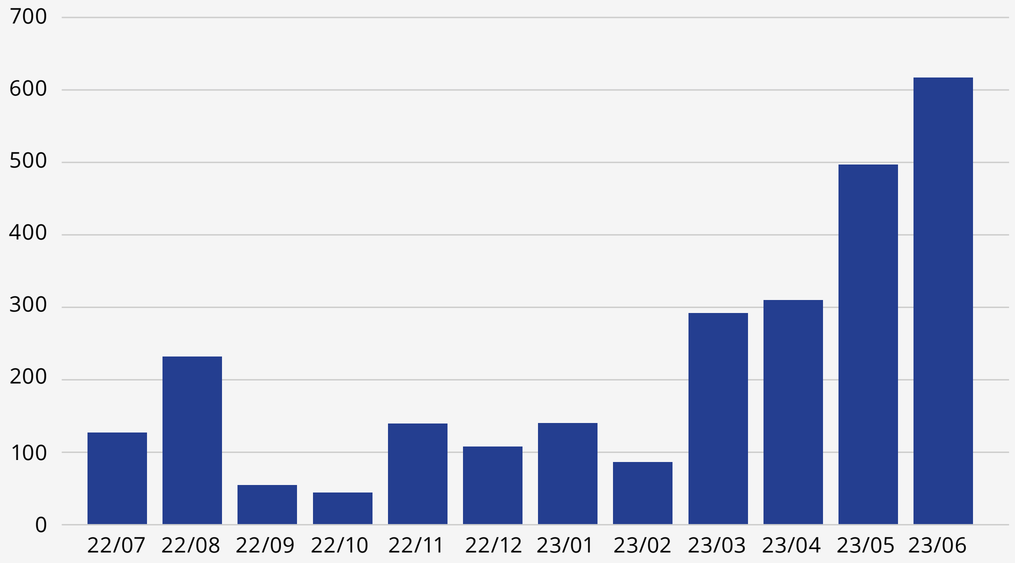
EUROPE

In October 2023, in its Threat Landscape Report[25] the European Union Agency for Cybersecurity (ENISA) echoed the global reports and trends. "In the latter part of 2022 and the first half of 2023," it said, "the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences." Hacktivism has expanded with the emergence of new groups, while ransomware incidents surged in the first half of 2023 and showed no signs of slowing down.

The top four threats were ransomware, malware, social engineering, and threats against data. Social engineering attacks grew significantly in 2023 with Artificial Intelligence (AI) and new types of techniques emerging. Within a more sophisticated landscape, phishing remains the top attack vector.

[23] https://www.pwc.com/ca/en/services/consulting/cybersecurity-privacy/cyber-threat-intelligence/year-in-review.html
[24] https://www.bleepingcomputer.com/news/security/canadian-government-discloses-data-breach-after-contractor-hacks/
[25] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA THREAT LANDSCAPE - OCTOBER 2023



The report identified public administration as the most targeted sector, followed by targeted individuals, health, digital infrastructure, and manufacturing, finance, and transport.

In Europe, the ongoing war of aggression against Ukraine has played a significant factor in shaping the cybersecurity landscape. Attacks have increased by 300% in NATO countries in the course of the war; a significant spike in spear-phishing activity targeting NATO countries was also observed by the Google threat analysis group[26], which noted that “Threat actors send email lures with themes related to the conflict, including humanitarian assistance and various types of fundraising. These emails are primarily used for scam activity but have also delivered a variety of threats.” CrowdStrike reported on credential phishing operations targeting government research labs, military suppliers, coordination companies and non-governmental organizations (NGOs) from August 2022 onward.[27]

BENELUX

On August 2, 2023, the Public Center for Social Action (CPAS) in Charleroi, Belgium, announced that its social branches had been closed by a ransomware attack.[28] CPAS institutions operate in each of the country’s 581 municipalities, providing social services to the local community including financial assistance, housing, medical and legal advice.

The institution’s spokesperson, Didier Neirynck, stated that its debt mediation service and Energy House service would also be closed as a result of the attack.

The report noted that cyber attacks on Belgian institutions have been occurring at a similar level to most other European nations in the past few years, with a hospital in Brussels — also the capital of the European Union and NATO Headquarters — being forced to divert ambulances after an incident in March.

In September 2023, cybercriminals breached the IT systems of the International Criminal Court (ICC) in the Netherlands. On September 20, the ICC said in a statement that “The evidence available thus far indicates a targeted and sophisticated attack with the objective of espionage.”[29]

While the ICC is still investigating the attack, ICC prosecutors are currently said to be investigating 17 cases in Ukraine, Uganda, Venezuela, Afghanistan, the Philippines, and Russia.

[26] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
[27] https://www.crowdstrike.com/global-threat-report
[28] https://therecord.media/charleroi-belgium-cpas-cyberattack
[29] https://www.infosecurity-magazine.com/news/icc-september-breach-was-espionage/

GERMANY

In November 2023, a massive ransomware attack hindered services in 70 German municipalities, paralyzing local government services in multiple cities and districts in western Germany.

In November 2023, an unknown hacker group encrypted the servers of a local German municipal service provider. To prevent the malware from spreading, the company restricted access to its infrastructure for over 70 municipalities, primarily in the western German state of North Rhine-Westphalia. The attack left local government services "severely limited," the company said in a statement posted on a temporary website, as its main site is inaccessible following the incident.

Nearly all town halls in the region were impacted by the attack. A week later, many of the impacted municipalities' services remained unavailable and the websites of some cities were still down. In many cities, internal and external communication, including email and phone services, were mostly nonfunctional. Payments like salaries, social assistance, and transfers from the nursing care fund may be hindered by the attack.

THE UNITED KINGDOM

According to a dataset published by England's Information Commissioner's Office (ICO) in September 2023, reported ransomware attacks on organizations in the United Kingdom reached record levels last year, when criminals compromised data on potentially more than 5.3 million people from over 700 organizations.[30]

Security incident trends data released in November 2023 by the ICO, noted that there have been 10 ransomware attacks on England's central government in the first six months of this year — doubling the total number of successful attacks on Whitehall departments since records began in 2019.[31]

The ICO report mentions that data on the sex lives of up to 10,000 people was stolen from a British government department in one of the record number of ransomware attacks of the period. It is not known which department the information was stolen from, nor why the government was holding this data, which is defined by the Information Commissioner's Office (ICO) as "any data on a person's sex life which does not specifically relate to orientation or health," potentially including the use of dating apps and menstrual period trackers.

In January 2023, the Royal Mail fell victim to a ransomware attack at the hands of LockBit.[32] The group hacked into the UK's postal services' software and blocked all international shipments by encrypting files. Negotiations took place between the two sides, but two weeks later, LockBit set a ransom demand of $80 million, 0.5% of the company's revenue, an amount Royal Mail officials called "absurd" and refused to pay. LockBit apparently then published the files on the dark web, with the message: "Royal Mail need [sic] new negotiator."

On February 6, Royal Mail published an updated statement on their progress stating that they had almost restored all services and continued to work towards a full recovery.

In June 2023, Barts Health NHS Trust, the largest health trust in the UK, was hit by a ransomware attack by ALPHV, aka BlackCat. The attackers claim that 7TB of sensitive data in what is claimed to be the biggest breach of healthcare data in the United Kingdom.[33]

[30] https://therecord.media/ransomware-attacks-record-in-UK

[31] https://therecord.media/sex-life-data-uk-government-ransomware-attacks

[32] https://www.theguardian.com/business/2023/feb/15/under-no-circumstances-will-we-pay-that-absurd-amount-royal-mail-tells-hackers

[33] https://techcrunch.com/2023/07/10/uk-hacks-public-sector-nhs-ransomware/

Some personally identifiable information belonging to workers has already been leaked by the ransomware gang on its website as proof of the intrusion and exfiltration, including people's financial details, CVs, and copies of passports and driving licenses.

As one of hundreds of NHS trusts in the country, Barts manages five hospitals in the capital and says it serves about 2.5 million people. The attackers claim to have other confidential documents of citizens, but it is not clear if or how much patient or medical data is involved.

As of the last report, the trust was still investigating the scope of the attack.

On August 8, 2023, the UK Electoral Commission issued a public notification that its database had been breached and the personal data of approximately 40 million people exposed.[34] The incident was identified in October 2022. Among the possible data exposed, the Commission lists personal data in the system, including name, email, home address, contact phone number, and "content of the webform and email that may contain personal data."

On September 14, 2023, Digital ID, the company responsible for numerous printing services for the Metropolitan Police Service of London's warrant cards, suffered an IT breach which may have exposed 47,000 officers' details. While it was originally reported by the Metropolitan Commissioner, in September also impacted the Greater Manchester Police, putting more than 20,000 police officers' details at risk.[35]

APAC

In 2022, Asia-Pacific (APAC) was the most attacked region globally, accounting for 31% of attacks globally.[36] By the second quarter of 2023, attacks in the region were up 22% year-on-year. In June 2023, the World Economic Forum (WEF Forum) called the Asia-Pacific Region the new "ground zero" for cyber attacks.[37]

The increase can be primarily attributed to the rapid digital transformation of the region; vital economic sectors have grown more vulnerable in the face of technological expansion. Southeast Asia's digital economy is growing by 17% annually,[38] driven by e-commerce, digital payments, e-learning, and remote work without a commensurate bolstering of cybersecurity.

In June 2023, Cloudflare released a report, "Securing the Future: Asia Pacific Cybersecurity Readiness Survey", based on the findings of a double-blind survey conducted in July 2023 of 4,009 leaders responsible for cybersecurity in their organizations from 14 markets, including Australia, China, Hong Kong SAR, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam. 78% of those interviewed had experienced at least one cybersecurity incident in the previous 12 months.

Of these, 80% reported four or more incidents, and 50%, 10 or more. Around 63% put the financial impact of cyber incidents on their organizations in the previous 12 months at a minimum of $1 million, with 14% saying their losses had exceeded $3 million.

Within the public sector, 79% of those in education, 70% in transportation, and 69% in government has experienced at least one cyber attack in the past year. In the face of rising frequency of attacks, only 38% of the cybersecurity managers surveyed by Cloudflare described their organizations as being well prepared to deal with cyberthreats. Healthcare, education, the public sector, and tourism had the highest percentages of managers who said they were unprepared to repel cyber attacks.

[34] https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems
[35] https://www.prolificnorth.co.uk/news/metropolitan-police-staff-data-at-risk-after-ransomware-attack-at-stockport-printer/
[36] https://www.ibm.com/reports/threat-intelligence
[37] https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/
[38] https://www.kearney.com/service/digital/article/-/insights/building-an-internet-for-the-future-of-southeast-asia

AUSTRALIA

Australian government agencies have become a growing target for cyber attacks worldwide, with a new Blackberry report released on November 29, 2023, revealing attempts to steal official information have soared by more than 60%. The country recorded one of the world's biggest quarterly rises in attacks against government departments, agencies and third parties in 2023, with public service attacks rising from 30,000 between March and May to 48,000 between June and August.[39] The attack with the highest destructive impact against the public sector occurred in April 2023, when Australian law firm HWL Ebsworth suffered a ransomware attack by the Russian-linked ALPHV/BlackCat ransomware group. In September 2023, the attackers published 1.1TB of the data it claimed to have stolen. It was later established that the group had exfiltrated 3.6TB worth of data from the firm. In total, around 2.5m documents were taken, with about 1m posted on the dark web.

HWL Ebsworth provided legal services and advice, sometimes on sensitive areas of work, for the Australian Defence Department, Home Affairs, the Australian federal police, Prime Minister and Cabinet, Services Australia, the Fair Work Ombudsman, and the Office of the Australian Information Commissioner.[40] On September 18, Australia's new cybersecurity coordinator, Darren Goldie, confirmed that sensitive and personal government information had been posted online by the ransomware group, and that at least 65 government agencies had been caught up in the attack.[41]

JAPAN

In the 2023 Global State of Cybersecurity Study[42] of 13 global markets, Japanese organizations experienced by far the lowest rate of data breaches of any country surveyed, 26% compared to the average breach rate of 60%. However, at $3.1 million USD, the average cumulative cost of those breaches was 60 percent higher than the global average.

According to the report, "The relatively low rate of data breaches may be associated to some degree with the relatively low adoption of work-from-anywhere initiatives in Japan compared with other countries, even during the COVID-19 pandemic. Subsequently, Japanese organizations were also less likely to expand mobile device deployments for remote workers, compared with those in other countries. It is worth noting that of successful breaches in Japan, 42% originated with a remote, employee-owned endpoint."

The majority of ransomware attacks in Japan have targeted its manufacturing sector; even their most notable attack in the public sector primarily affected the transport of manufactured goods.

In July 2023, the Port of Nagoya, which handles almost 10% of Japan's trade volume, experienced a significant disruption as a result of a LockBit ransomware attack that brought container operations across all its terminals to a standstill for several days. The disruption caused considerable operational delays and sent economic shockwaves throughout Japan's complex supply chain.[43] Cargo trucks crowded the port when it became impossible for trucks to load or unload containers.

The Port of Nagoya has been the biggest port in Japan in terms of annual cargo volume since 2002. The port handles an average of 10,000 pieces of cargo per day, according to the association.[44] The group said it did not pay the ransom.

[39] https://www.themandarin.com.au/235644-criminals-target-government-with-record-cyber-attacks/

[40] https://www.theguardian.com/technology/2023/jul/05/hwl-ebsworth-hack-russian-gang-released-sensitive-personal-and-government-information-australian cybersecurity-chief-says

[41] https://www.theguardian.com/australia-news/2023/sep/18/hwl-ebsworth-hack-65-australian-government-agencies-affected-by-cyber-attack

[42] https://blogs.infoblox.com/security/2023-global-state-of-cybersecurity-study-japan/

[43] https://www.japantimes.co.jp/news/2023/07/06/national/nagoya-port-hack-resume-operations/

[44] https://www.moj.go.jp/content/001398997.pdf

SOUTH KOREA

In May 2023, South Korean law enforcement disclosed that hackers had breached the Seoul National University Hospital and stolen confidential medical data. The breach occurred in mid-2021, followed by a two-year investigation. Media sources alleged that the Kimsuky APT group perpetrated this attack. The police said the incident resulted in data exposure for 831,000 individuals, most of whom were patients. 17,000 of the impacted people are current and former hospital employees.[45]

In July 2023, a South Korean government-affiliated institution fell victim to a Business Email Compromise scandal that resulted in a loss of 175 million won, or $131,000. This was reportedly the first such incident against a South Korean government public organization. According to Korean media reports, the Korea Institute of Startup and Entrepreneurship Development (KISED), operating under the Ministry of SMEs and Startups, was transferring payment to a partner in Europe when the email between the partners was intercepted and the senders deceived into sending the funds to the hackers instead.[46]

In August 2023, threat actors attempted to compromise a joint U.S.-South Korean military exercise on countering nuclear threats from North Korea. The hackers, believed to be linked to a North Korean group that researchers call Kimsuky, carried out their hack via several spear phishing emails to South Korean contractors working at the South Korea-U.S. combined exercise war simulation centre, the Gyeonggi Nambu Provincial Police Agency said in a statement. South Korean police said no classified information had been compromised.

MALAYSIA

In May 2022, the Malaysia New Straits Times reported the theft and publication of 22.5 million personal records of citizens born between 1940 and 2004, purportedly stolen from the National Registration Department (NRD).

Local tech portal Amanz reported that the database, 160GB in size, was being sold for US$10,000 on the dark web. It was claimed that the data was siphoned from the NRD through a data-sharing platform that is used by numerous Malaysian government agencies.[47]

Malaysia's Home Minister Hamzah Zainudin said the alleged data leak did not come from the NRD, but from "several agencies which we have given some leeway for them to obtain information from us".

In December 2022, more suspected data leaks were reported by local media, including one that involved almost 13 million accounts from the country's satellite television and IPTV provider, the Election Commission of Malaysia, and Maybank, the country's popular online banking service. These reports led to Communications and Digital Minister Fahmi Fadzil calling for CyberSecurity Malaysia and the Personal Data Protection Department to launch further investigations. All three organizations claimed that the data leak allegations were false.[48]

In 2023, Malaysia has recorded its highest number of data breach cases to date. In September 2023, Palo Alto Networks' 2023 State of Cybersecurity ASEAN noted that Malaysia had the highest incidence of disruptive cyber attacks within ASEAN over the past year.[49] One-third of Malaysian organizations reported a 50% or more increase in cybersecurity incidents.

[45] https://www.bleepingcomputer.com/news/security/north-korean-hackers-breached-major-hospital-in-seoul-to-steal-data/
[46] https://www.koreatechdesk.com/cyber-attack-hits-south-korean-government-institution-resulting-in-loss-of-135000-usd-to-phishing-scam/
[47] https://www.straitstimes.com/asia/se-asia/data-of-225-million-malaysians-born-1940-2004-allegedly-being-sold-for-us10k
[48] https://www.darkreading.com/cybersecurity-analytics/black-hat-asia-2023-cybersecurity-maturity-concern
[49] https://cybersecurityasean.com/daily-news/malaysias-cybersecurity-wake-call

The report noted that the critical infrastructure sector appears to be the prime target, amplifying the urgency for robust cybersecurity measures to safeguard essential services, and that the government sector faces the second highest threat level in 2023.[50]

FORTIFYING THE DEFENSES AGAINST CYBER ATTACKS

According to numerous reports and summarized by KnowBe4's Roger Grimes, data-driven defense evangelist, 70 to 90% of ransomware attacks are the result of social engineering and phishing. Fortifying the most vulnerable link in the cybersecurity layer – the human – can be the most cost-effective way to help organizations better protect themselves against the rising wave of attacks in the public sector.

SECURITY AWARENESS TRAINING AND TESTING

People who are unaware of security threats are much more susceptible to becoming a victim of them. People who lack awareness of organizational processes for reporting cybersecurity threats will not become a part of the last line of an organization's defense.   Security awareness training—and the integral simulated phishing testing component of modern training—mitigates both challenges.

There are various aspects of security awareness training, which includes training campaigns to inform and educate staff, delivered continuously in consumable formats for employees to strengthen security culture at their organizations and beyond. For example, modern security awareness training uses posters, video case studies, and content for email campaigns to strengthen the human layer of defense against phishing, BEC, data breaches, privacy invasions, and more.

The testing side of security awareness training provides an ongoing mechanism for ascertaining the efficacy of training, along with the likelihood that attacks will be successful. The purpose of phishing testing is to enable employees to safely cultivate necessary skepticism and reflexes to ultimately protect the organization from real-world attack scenarios.

KnowBe4 is the provider of the world's largest security awareness training and simulated phishing platform. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. The late Kevin Mitnick, an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

[50] https://www.darkreading.com/cybersecurity-analytics/black-hat-asia-2023-cybersecurity-maturity-concern

Additional Resources

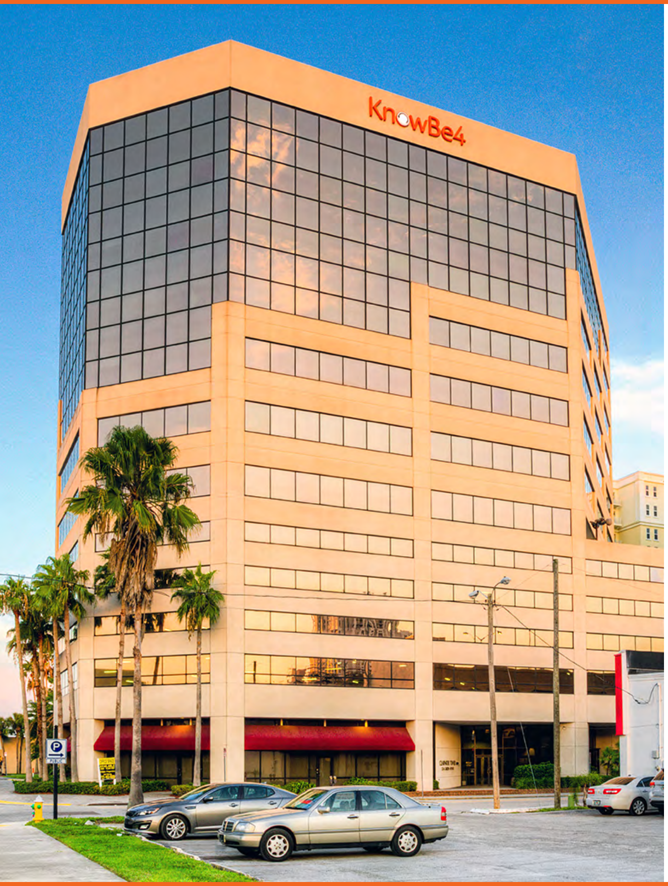
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organisations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognised cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organisations rely on KnowBe4 to mobilise their end users as their last line of defence and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com