2018 Cyber Incident & Breach Trends Report

Review and Analysis of 2018 Cyber Incidents and Key Trends to Address

Released 9 July 2019

OTA
Online Trust Alliance
an **Internet Society** initiative

Table of Contents

2018 – Some Better, Some Worse, All Bad

Looking at some of the statistics it might seem that 2018 finally brought some cyber incident relief – the number of data breaches and exposed records were down, and both ransomware and DDoS attacks were down overall. Yet the financial impact of ransomware rose by 60%, losses from business email compromise (BEC) doubled, cryptojacking incidents (the unauthorized use of others' computing resources to conduct cryptomining) more than tripled, and there continued to be a steady stream of high-profile data breaches.

It is difficult to get a complete, accurate picture of the overall cyber incident landscape. Much like putting together a jigsaw puzzle with only a handful of key pieces, it is possible to get a sense of the overall picture, but many of the details are missing. In tracking cyber incidents, many key data "pieces" exist, but are limited for a variety of reasons – they often represent only one vendor's view of their user base, they are typically regional and not global, it is easier to measure attacks than measure which are successful, there is a lack of consolidated reporting mechanisms, and finally, it is still the case that most incidents go unreported.

In this context, the approach taken in this year's report is to lay out the various key statistics and trends across the types of cyber incidents, but not come to a definitive conclusion regarding a precise number of incidents. As in prior years, the report will still outline threat trends and how to address them.

There are several organizations that track data breaches, mostly relying on public reports, though the results vary widely due to different methodologies. Risk Based Security reports the highest number at 6,515 breaches and 5 billion exposed records, both down from 2017.[1] Identity Theft Resource Center also reports on breaches, finding 1,244 in 2018 with approximately 2 billion exposed records – the number of breaches is down from 2017 while the number of *sensitive* records exposed (447 million) is up significantly.[2] Privacy Rights Clearinghouse reported 635 breaches and 1.4 billion exposed records in 2018, both down from 2017.[3] Though these reports do include some international breaches, they do not cover all breaches worldwide, as shown in DLA Piper's GDPR Data Breach Survey, which surveyed data protection authorities in the EU and found 59,000 reported breaches just between May and December 2018.[4]

2018 Incident Highlights

95% of breaches could have been prevented (ISOC)

3.2% decrease in reported breach incidents (RBS)

5 billion records exposed, a 35.9% decrease (RBS)

$8 billion financial impact of ransomware (CV)

12% rise in business targeted ransomware (Symantec)

$12.5 billion in global EAC/BEC losses since 2013 (FBI)

Worldwide estimates. Sources: (ISOC) Internet Society, (RBS) Risk Based Security, (CV) Cybersecurity Ventures

[1] https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report
[2] https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf
[3] https://www.privacyrights.org/data-breaches
[4] https://www.dlapiper.com/~/media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf

In 2018 there certainly were many high-volume (and therefore high-profile) breaches – a dozen exposed more than 100 million records – and they can be instructive from both a trend and lessons learned standpoint. The largest breach, which involved 1.1 *billion* records of Aadhaar, India's national ID database, happened early in the year and was attributed to an unsecured API.[5] The Marriott/Starwood breach impacted 383 million people. In retrospect it was clear that attackers had been in the Starwood network since 2014 (pre-Marriott acquisition), and would have been detected by routine network checks, thus highlighting the need to perform regular security checks and due diligence.[6] [7] Under Amour had a breach of 150 million MyFitnessPal records and was lauded for its rapid and thorough response, though it was revealed that some passwords were encrypted using the weak SHA-1 hash.[8]

Finally, the Facebook/Cambridge Analytica "breach", which impacted 87 million people, brought into the public discourse questions regarding appropriate protection, use and access to user data.[9] This sampling of top breaches runs the gamut in terms of learning opportunities – from securing third-party access (both technically and from a privacy practice standpoint), to ongoing diligence in monitoring for vulnerabilities and unauthorized access, to keeping only necessary data and securing it properly.

Ransomware was a major attack vector in 2017, and while it continued to have an impact in 2018, the overall numbers declined during the year. In its Internet Security Threat Report (ISTR) 24, Symantec reported more than 500,000 ransomware infections, which was down 20% overall from 2017, but they saw a shift toward enterprise users, which actually grew 12%.[10] Many reports hypothesize that attackers shifted to other methods such as cryptojacking where the payback was more certain and exposure was less likely. Still, ransomware continues to make headlines, especially when it cripples organizations such as the city of Atlanta, which has spent an estimated $17 million to handle the aftermath.[11] In fact, Cybersecurity Ventures estimates that ransomware will cost organizations $8 billion in 2018, growing to $20 billion in 2021.[12]

Cryptojacking became prominent in late 2017 as the price of cryptocurrency soared.[13] If an attacker can infiltrate an organization, they have many choices regarding how to use that access, and planting code that quietly uses computing resources to mine cryptocurrency is certainly one approach. Though on the surface such attacks may seem innocuous, there are real costs associated with extra energy use, sluggish performance (in which case computers might be upgraded unnecessarily, giving attackers even more resources to work with), and even failures of equipment due to heavy use. Attackers have even gone to the

[5] https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/
[6] https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/
[7] https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/
[8] https://threatpost.com/under-armour-reports-massive-breach-of-150-million-myfitnesspal-accounts/130863/
[9] https://www.vice.com/en_us/article/3kjzvk/facebook-cambridge-analytica-not-a-data-breach
[10] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
[11] https://www.databreachtoday.com/atlantas-reported-ransomware-bill-up-to-17-million-a-11281
[12] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
[13] https://www.wired.com/story/cryptojacking-took-over-internet/

point of infecting websites or ads in order to utilize users' browsers (and thereby their computers) to expand the available computing resources.[14] [15]

Trend Micro detected more than 1.3 million instances of cryptojacking code in 2018, a greater than three-fold increase from 2017.[16] Many reports cite evidence that cryptojacking attacks declined as 2018 progressed, in line with the falling value of cryptocurrency, but it is important to remember that these attackers have a foothold and can pivot to other, more lucrative forms of attack.

Distributed Denial of Service (DDoS) attacks were reported to have declined slightly in 2018, though they are still wreaking havoc in many industries. Kaspersky Labs reported a 13% decline in attacks in 2018, to approximately 160,000, while NSF Focus reported similar numbers, estimating 148,000 DDoS attacks for the year.[17] [18]

The challenge with DDoS is determining how many attacks are successful – there is no aggregated reporting and most organizations are reluctant to acknowledge their vulnerability. However, there are examples of successful attacks across a wide range of industries, ranging from banking (ABN AMRO) to education (Infinite Campus) to email services (ProtonMail) to software services (GitHub, the largest recorded DDoS attack to date).[19] [20] [21] [22] Netscout estimates that the cost of downtime averages nearly $222,000 per attack.[23]

Another form of attack – supply chain attacks – grew significantly in 2018. High-profile historical examples are the Target breach in 2013 where access was gained via a Heating, Ventilation and Air Conditioning (HVAC) vendor, the NotPetya attack in 2017 where an update to accounting software was infected and then spread widely, and the CCleaner attack in 2017 where more than 2 million infected copies of the popular computer cleanup tool were downloaded. One of the most prevalent forms seen in 2018 was "formjacking," where attackers infect a website's submission form via a third-party supplier or malicious code carried in ads, and then either scrape the information or infect the user. Symantec's ISTR reported a 78% growth in supply chain attacks and estimates that nearly 5,000 websites a month contained formjacking code. The most prominent 2018 example of this type of attack was Magecart, which infected Ticketmaster, British Airways, Newegg and 800 others.[24] [25]

[14] https://mashable.com/2018/01/27/coinhive-youtube-google-doubleclick/
[15] https://www.wired.com/story/make-a-wish-website-cryptojacking-hack/
[16] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unraveling-the-tangle-of-old-and-new-threats
[17] https://securelist.com/ddos-attacks-in-q4-2018/89565/
[18] https://nsfocusglobal.com/2018-ddos-attack-landscape/
[19] https://www.abnamro.com/en/newsroom/newsarticles/2018/ddos-attacks.html
[20] https://www.infosecurity-magazine.com/news/ddos-attacks-infinite-campus/
[21] https://techcrunch.com/2018/06/27/protonmail-suffers-ddos-attack-that-takes-its-email-service-down-for-minutes/
[22] https://techcrunch.com/2018/03/02/the-worlds-largest-ddos-attack-took-github-offline-for-less-than-tens-minutes/
[23] https://www.netscout.com/report/
[24] https://www.securityweek.com/new-magecart-group-targets-french-ad-agency
[25] https://www.riskiq.com/blog/labs/magecart-adverline/

Business Email Compromise (BEC), also known as Email Account Compromise (EAC), attacks also grew significantly in 2018. In this attack, employees of organizations are deceived into sending funds (or equivalent, such as gift cards) as a response to emails from attackers pretending to be vendors or executives. The FBI, via its Internet Crime Complaint Center, collects reports on these incidents. In their 2018 Internet Crime Report they reported more than 20,000 BEC/EAC incidents in the U.S., resulting in nearly $1.3 *billion* in losses (an increase from approximately 16,000 incidents and $677 million in losses in 2017).[26] Their report in mid-2018 looked at total global BEC/EAC incidents since 2013 and reported nearly 80,000 incidents representing a total of $12.5 *billion* in losses. In response, in addition to filtering out suspect messages, many organizations are marking messages that originate from outside the organization as “External” and are conducting extensive training for employees.

An attack vector that also gained steam in 2018 was “credential stuffing,” wherein attackers use the large database of breached credentials to gain access to users' accounts.[27] [28] In early 2019, several database compilations totaling more than 2 billion credentials were discovered, and Akamai reported 30 billion credential stuffing login attempts for 2018, highlighting the scale of the problem.[29] [30] According to research by Shape Security, only approximately 1% of these attacks are successful, but given the scale of the attacks, this still has an estimated impact of more than $5 billion per year.[31] High-profile victims of credential stuffing in 2018 were HSBC, Nest, Dunkin Donuts, Reddit, DailyMotion and TurboTax.[32] [33] [34] [35] In response, there has been a general call for users to use unique passwords for each service (e.g., via a password manager) and to enable multi-factor authentication where possible.

Looking across the cyber incident landscape, a rough estimate of the overall volume can be calculated. The lead categories are cryptojacking (1.3 million) and ransomware (500,000), followed by breaches (60,000), supply chain (at least 60,000 infected websites), and BEC/EAC (20,000). Credential stuffing and DDoS attack success rates are more difficult to determine, though there are significant known successes for both. Adding it all up, the Internet Society's Online Trust Alliance estimates that there were more than 2 million cyber incidents in 2018, and it is likely that even this number significantly underestimates the actual problem.

The financial impact across all these types of incidents is also difficult to determine. While some have definitive reports (BEC/EAC at $1.2 billion in 2018) or strong estimates (ransomware at $8 billion, credential stuffing at $5 billion), others have more general estimates (average cost of data breach grew to $3.86 million according to Ponemon Institute, average cost of $222,000 per successful DDoS attack), and some are

[26] https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf
[27] https://www.wired.com/story/what-is-credential-stuffing/
[28] https://www.zdnet.com/article/an-inside-look-at-how-credential-stuffing-operations-work/
[29] https://www.wired.com/story/collection-leak-usernames-passwords-billions/
[30] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-attacks-and-economies-report-2019.pdf
[31] https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape_Credential_Spill_Report_2018.pdf
[32] https://www.zdnet.com/article/hsbc-discloses-security-incident/
[33] https://www.zdnet.com/article/dunkin-donuts-accounts-compromised-in-second-credential-stuffing-attack-in-three-months/
[34] https://www.wired.com/story/nest-cameras-pew-die-pie-north-korea-passwords/
[35] https://www.zdnet.com/article/dailymotion-discloses-credential-stuffing-attack/

undetermined (cryptojacking, formjacking).[36] Even using these loose estimates, it is easy to justify a total impact of more than $45 billion in 2018.

All of this begs the question "are things getting better or worse"? The answer is "both" – as some types of attacks wane, others rise. What is very clear is that there are too many cyber incidents creating an unacceptable level of financial impact. As the following sections will outline, addressing these threats comes back to a basic set of core best practices that require discipline to implement and maintain.

Existing Trends

Each year this report highlights trends we see in cyber incidents, as well as emerging trends. We have covered the following trends in prior reports, and though they continue to be significant factors in the cyber incident landscape, they no longer represent the leading edge:

- **Ransomware** occurrences saw a slight decline in 2018, though total losses continue to rise. While attacks overall might be down slightly, other research indicates troubling trends in specific types of attacks. Researchers at Recorded Future noted an increase in reported ransomware attacks against state and local governments[37] in 2018 and early 2019. Recorded Future also noticed, interestingly, that state and local governments were the least likely to pay the ransom compared to other types of organizations hit by ransomware.

- **Cyber insurance** continues to be one way that organizations can protect themselves from the impact of cyber incidents. According to Fitch Ratings the cyber insurance industry in the U.S. grew 8% in 2018 to approximately $2 billion in payouts. This growth was down from 37% in 2017, which according to Fitch is a sign that the cyber insurance market is maturing.[38]

- **Cloud services** are an increasingly important part of the IT infrastructure for most organizations. Cloud services offer many benefits such as increased security, but they also come with a downside since proper security configuration is the responsibility of the end user. One estimate by research firm Digital Shadows found that in 2018 there were 1.5 billion files exposed around the world solely due to misconfigurations in cloud services.[39] In addition, one cloud security company, Armor, estimated cloud users suffered $681 million in losses due to cloud attacks. But this is only based on their own customer base, so presumably the total is far higher.[40]

- **IoT devices** are a clear attack vector that, in theory, can be used to perpetrate several of the types of attacks mentioned above – from cryptojacking to DDoS to ransomware. As a result, attacks utilizing IoT devices are included in virtually every cyber incident number mentioned above, though

[36] https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/
[37] https://www.recordedfuture.com/state-local-government-ransomware-attacks/
[38] https://www.insurancejournal.com/news/national/2019/05/15/526467.htm
[39] https://info.digitalshadows.com/FileSharingDataExposureResearch-Press.html
[40] https://www.darkreading.com/attacks-breaches/cloud-customers-faced-681m-cyberattacks-in-2018/d/d-id/1333721

pinning down the specific contribution related to IoT is difficult. Still, since many of the IoT device vulnerabilities continue to be related to simple items such as default passwords, insecure software or unencrypted communications, IoT manufacturers can take basic steps to properly secure IoT devices using principles in the Internet Society's Online Trust Alliance IoT Trust Framework.[41] In one prominent 2018 IoT episode, the FBI advised that users of certain types of routers should restart them after Cisco researchers discovered 500,000 routers were compromised by malware.[42] Another way to assess the scope of the problem is to track how many types of malware are designed for IoT devices. Kaspersky Labs reported that in the first half of 2018 they saw a three-fold increase in the number of malware variations used to attack IoT devices.[43]

Regulatory Shifts – In recent years, there has been a surge in legislative and regulatory government activity around the world related to organizations' obligation to properly protect user data. Many of these are still in process so it is critical for organizations to stay abreast of the laws and regulations that apply to the jurisdictions where they have users. With the EU General Data Protection Regulation (GDPR) now in full effect, the first data breach fines began to be discussed in European Data Protection Authorities. For example, Facebook is facing a possible fine of $1.6 billion from the Irish Data Protection Authority for allegedly mishandling user data resulting in the breach of over 50 million users' personal data.[44] In the United States many states are passing, or are considering passing, laws with similar provisions. Vermont, for example, passed a new law to regulate data brokers in the state which includes protecting user data.[45]

Emerging Trends

In addition to the trends we have covered in the past, this year we look at three emerging attack types that rose to prominence in 2018. While these are also not truly "new", we felt that their growth warranted a deeper look.

Mining Your Device

Cryptocurrency is an increasingly valuable commodity, with large institutions like JP Morgan Chase getting into the game in 2019 and Facebook announcing that it was creating its own cryptocurrency.[46] [47] In conjunction with the prevalence of cryptocurrency came the rise of cryptojacking. This is a specific type of attack aimed at hijacking devices to harness computing power at scale to efficiently mine cryptocurrency.

[41] https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/
[42] https://www.securitynewspaper.com/2018/05/31/fbi-launches-international-alert-cisco-routers-easy-hack/
[43] https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018
[44] https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation
[45] https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/
[46] https://www.theverge.com/2019/2/14/18224976/jp-morgan-chase-cryptocurrency-banking-cnbc
[47] https://www.wsj.com/articles/facebooks-libra-cryptocurrency-how-it-stacks-up-to-bitcoin-and-paypal-11561714204

This type of attack involves installing malware on a device connected to the Internet, which could be virtually anything from a phone, to a game console, to an organization's servers. The attacker then uses the devices' computing power to "mine" cryptocurrency.

For context it is useful to explain, in the most basic terms, how cryptocurrency is mined. There are thousands of active cryptocurrencies on the market today, but one of the oldest and most recognizable is Bitcoin, so we will use Bitcoin as an example of how cryptocurrency is mined.

In short, mining cryptocurrency involves using a device's processing power to earn, in this example, Bitcoins. Bitcoins can then be exchanged for other currency such as Euros. Initially, regular users could use their home computers to mine bitcoins, though over time the processing power it takes to earn Bitcoins has risen significantly and as a result most cryptocurrency is now mined by professional operations running large server farms. Put another way, it currently takes far more processing power than most individual users have access to in order to efficiently mine Bitcoins.[48]

Because of large centralized cryptomining operations, those without access to that level of resources began looking for other ways to obtain the processing power needed to efficiently mine cryptocurrency – enter cryptojacking.

The goal of any cryptojacking operation is to hijack enough devices so that their processing power can be pooled. This is achieved by hijacking vast numbers of devices, but only using small amounts of each individual device's processing power, so the user is not likely to notice their device is being hijacked. Conceptually similar to a botnet, attackers then network these hijacked devices together to mine cryptocurrency.

As noted by Malwarebytes, the initial form of this attack came through web browsers.[49] Attackers would install malicious code on a website and when a user visited that site the attacker would use that code to run a background process to mine cryptocurrency while that user was visiting that site. While Malwarebytes notes that this type of cryptojacking has decreased recently, it is also clear that cryptojacking has morphed into hijacking everything from Android phones through malicious apps to entire organization networks.[50] [51]

As noted above it is extremely hard to measure the actual number of cryptojacking incidents, but they at least tripled in 2018. Despite this type of attack being relatively new, the ways to avoid this type of attack for both consumers and organizations are basically the same as any other attack. Use unique passwords and multi-factor authentication, monitor for anomalous activity on the network, be sure any software installed on a device comes from a reputable source and that the software is fully patched. See our readiness tips below for more information on how to avoid these attacks.

[48] https://www.marketwatch.com/story/if-youre-mining-bitcoin-from-home-youre-now-losing-money-2018-10-12
[49] https://blog.malwarebytes.com/cybercrime/2019/05/cryptojacking-in-the-post-coinhive-era/
[50] https://news.sophos.com/en-us/2018/09/24/cryptojacking-apps-return-to-google-play-market/
[51] https://www.zdnet.com/article/this-new-cryptomining-malware-targets-business-pcs-and-servers/

More Stuffing? No Thanks.

As mentioned earlier, credential stuffing came to the fore in 2018. Given that there are now more than 2.2 billion breached credentials in play, attackers are using known username/password pairs and commonly used passwords to gain access directly to accounts across a wide range of industries. As described in Akamai's State of the Internet/Security report, the network profile of these attacks can look similar to botnets – they saw more than 30 billion login attempts attributed to credential stuffing in 2018, three days peaked at more than 250 million attempts and just in the retail sector the average was 115 million attempts per day from May through December.[52]

Several high-profile attacks occurred in 2018, and though many were initially believed to be breaches, they turned out to be brute-force credential attacks. What can be done to protect against these attacks? First, it should be recognized that the success of these attacks is largely based on sloppy password management practices by users – they either reuse passwords across multiple sites or use common passwords that are easy to guess. Security researcher Troy Hunt has a service called Pwned Passwords where users can enter their password(s) to see if they match any of the more than 550 million breached passwords.[53]

Organizations can use this database to verify that users' passwords are not on the breached list and force users to change them to strong, non-compromised passwords, as Nest seemed to do even for existing accounts.[54] They can also institute login policies that have rate limiting, and limit the number of login attempts allowed before freezing access. Finally, they can implement multi-factor authentication so that a password isn't the only credential required for access. Users should not reuse passwords across services and ensure that their passwords are strong (this is easily accomplished through use of a password manager). Users should also enable multi-factor authentication wherever possible to add another layer of protection to account access.

Who Can I Trust? No One.

Supply chain attacks – wherein attackers infiltrate via third-party website content, vendors' software or third-parties' credentials – are not new (think Target in 2013, CCleaner and Not Petya in 2017), but they continue to proliferate and take on different forms. Symantec reported a 78% increase in these types of attacks in 2018, CrowdStrike found that two-thirds of surveyed organizations had experienced such attacks at an average cost of $1.1 million, and Carbon Black estimates that half of all attacks involve the supply chain. [55] [56] [57]

[52] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-attacks-and-economies-report-2019.pdf
[53] https://haveibeenpwned.com/Passwords
[54] https://www.internetsociety.org/blog/2018/05/nest-alert-protection-from-pwned-passwords/
[55] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
[56] https://www.darkreading.com/attacks-breaches/two-thirds-of-organizations-hit-in-supply-chain-attacks-/d/d-id/1332352
[57] https://threatpost.com/half-all-attacks-supply-chain/143391/

The highest-profile supply chain attack in 2018 was Magecart, which infected credit card entry forms on at least 6,400 sites worldwide, mostly via third-party support tools and advertising.[58] [59] At first glance many of these attacks were thought to be database breaches at notable victims such as Ticketmaster, British Airways and Newegg, but upon further analysis were determined to be "formjacking".[60] News of these attacks continued in early 2019, with headlines involving Asus computers and video game makers.[61] [62] The Magecart attacks also continued, though likely by a different group, infecting more than 200 online campus stores via e-commerce platform PrismWeb.[63] Though the impact is still unclear, an attack implemented via analytics service Picreel and open-source project Alpaca Forms infected more than 4,600 websites and allowed attackers to collect payment information and passwords.[64]

In this environment, organizations clearly need to adopt a "trust no one" mentality and take steps to protect against these attacks, though it is difficult given the complexity of systems and the number of third parties involved. For third-party tools used on websites, this can be done by thorough testing of code (and especially any updates to it) in a sandboxed environment and monitoring for anomalous behavior. For code embedded in other applications a similar approach can be taken, including assurance that updates are signed and verified from the third party. For third parties that provide services and have credentialed access to an organization's systems, it is important to limit their access to only appropriate systems, and have processes in place to log changes and test updates. In all cases regular penetration testing should be performed to look for anomalies.

[58] https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/
[59] https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/
[60] https://www.itpro.co.uk/cyber-attacks/31992/british-airways-ticketmaster-and-newegg-hacks-part-of-massive-magecart
[61] https://www.pcmag.com/news/367369/hackers-infect-thousands-of-asus-pcs-via-malicious-updates
[62] https://www.wired.com/story/supply-chain-hackers-videogames-asus-ccleaner/
[63] https://www.bleepingcomputer.com/news/security/over-200-college-campus-stores-infected-with-card-stealing-scripts/
[64] https://www.zdnet.com/article/hackers-are-collecting-payment-details-user-passwords-from-4600-sites/

Readiness Guidance

This report offers guidance on what organizations can do to protect data. While the trends outlined above clearly show a shifting landscape of attack types, the advice we offer each year generally stays the same.

Attack types may change, but these principles will continue to help organizations protect themselves. The key point to understand is that these incidents will occur at some point and the responsibility of security is not limited to the IT department – it is the responsibility of everyone in the organization to remain vigilant and be aware of these principles.

Fundamentals

- All businesses collect some form of sensitive, valuable information. Cyber incidents will occur.
- Data stewardship, privacy and incident readiness are everyone's responsibility.
- Data management and privacy practices need continual review.
- Every organization needs to have a current, tested response plan.
- Ongoing employee training is a critical key to success.

Core Readiness Principles

As cyber incidents increase and evolve in sophistication, the cost and damage grow. Through the years, the leading incidents (and how they were handled) have taught important lessons:

1. **Responsibility for incident protection and readiness is organization-wide.** Data stewardship, security and associated privacy practices are the responsibility of the board, executives, all employees and all departments (not just IT).
2. **Data is an organization's most valuable asset.** Identify what you have, where it is, why and how you use it and the potential risks to your organization and individuals should it be inappropriately accessed, held hostage, released or erased.
3. **Only collect and retain data that has a business purpose for as long as it is needed**. Secure it while it's held; delete it when it's no longer needed. Criminals cannot steal or hold hostage data you don't have, and such minimization may be a regulatory requirement for your organization.
4. **The level of data security you apply must be commensurate with the data held.** The security in place should reflect the risk of damage to consumers and the organization should that information be inappropriately accessed. Organizations should develop a data minimization strategy including a classification matrix that guides how various types of data should be protected, stored and discarded across an organization.
5. **Protection involves not only the specific incident (data loss, ransom paid), but also the costs of business interruption.** This includes locked data, network and system interruption and connected device takeover.

6. **Have plan to reduce the impact of an attack**. An incident plan needs to incorporate training to help prevent, detect, mitigate, respond and recover. Just like first responders, employees must be regularly trained, equipped and empowered to deal with a data loss or other cyber incident. Planning is the key to maintaining trust and business vitality while helping to ensure business continuity. Developing key relationships ahead of time with attorneys, public relations, forensics, and identity protection firms is essential to maximizing the response effectiveness.
7. **Security and privacy are not absolutes and must evolve**. Organizations need to regularly review their procedures for collection, storage, use, management and security of all data (along with review of changing technologies, best practices and regulations).
8. **Security is beyond the organization's desktops, networks and walls**. Cloud services, third-party processors and external business partners expand the attack landscape. Conduct a risk assessment prior to partnerships or service agreements and periodically re-assess. Require regular (weekly, monthly, quarterly or annual) reports from vendors specifying their internal data security processes, data removal methods, tools and technology implementations and documentation. Vendors should also be encouraged to take advantage of independent audits and/or certification programs.
9. **Connected devices introduce new risk levels.** The rapid adoption of connected devices – from Smart TVs in the boardroom to coffee makers in the breakroom to employees' personal mobile devices and wearables connected to the office Wi-Fi – dramatically increase the threat landscape. Ongoing risk assessment of all IoT devices and the development and enforcement of an employee policy for connecting devices to the corporate network is critical since a single connected device can introduce threats network-wide.
10. **Build trust through transparency**. In the event of an incident, keep communication clear. Whether communicating with customers, board members or data protection authorities, keeping important stakeholders informed early with regular updates is a critical part of maintaining trust.

Top Level Incident Ready Checklist

- □ Complete risk assessments for executive review, operational process and third-party vendors
- □ Review security best practices and validate your organization's adoption or rationale for not adopting
- □ Audit your data and review your data stewardship practices, including data lifecycle management
- □ Complete a review of insurance needs including exclusions and pre-approval of coverage for any third-party services (such as cyber forensics, remediation provider, PR firm, etc.)
- □ Establish and regularly test an end-to-end incident response plan including empowering 24/7 first-responders
- □ Establish/confirm relationships with data protection authorities, law enforcement and incident service providers
- □ Review and establish forensic capabilities, procedures and resources (internal and third-party providers)
- □ Develop communication strategies and tactics tailored by audience (e.g., messages to employees vs. messaging to media vs. notifications to customers)
- □ Review remediation programs, alternatives and service providers
- □ Implement ongoing employee training for incident response
- □ Establish employee data security awareness and ongoing education on privacy, incident avoidance (password practices, how to recognize social engineering, etc.) and incident response
- □ Understand the regulatory requirements, including relevant international requirements

About the Internet Society's Online Trust Alliance (OTA)

The Internet Society's Online Trust Alliance (OTA) identifies and promotes security and privacy best practices that build consumer confidence in the Internet. Leading public and private organizations, vendors, researchers, and policymakers contribute to and follow OTA's guidance to help make online transactions safer and better protect users' data. The Internet Society is a global nonprofit dedicated to ensuring an open, globally connected, trustworthy, and secure Internet for everyone.

1907-1