TitanHQ

2020 Guide to Data Breach Prevention

As everyone moves into 2020, one undeniable concern that will continue from previous years is data privacy and protection. Data breach costs increased by 12% in 2019 and they continue to rise. According to IBM and Ponemon's research, the average cost of a data breach is $3.92 million, and over 1,200 data breaches were reported in 2019. It should be clear to any organization that cybersecurity is paramount for data security, but human error continues to be a primary difficulty for IT staff dedicated to creating a secure environment for employees and customers.

How Do Hackers Obtain Data?

Before diving into prevention, it's important to understand the ways hackers exploit vulnerabilities and find ways around current defenses. Not every bad actor is a high-end hacker finding low-level vulnerabilities on expensive equipment. Some attackers run freely available scripts they've downloaded from the public Internet.

Others use phishing and its variants (e.g. vishing and smishing) to exploit humans. Because phishing does not require advanced computer knowledge, it can be used by an attacker to steal credentials, drop malware on a critical office machine, or scan a network for important documents. Attackers have several tools at their disposal, but here are the top five reasons bad actors gain access to organization data.

1. Unpatched Outdated Software or Firmware

IT software and hardware vendors constantly release patches to remediate equipment vulnerabilities. However, it's up to organizations to apply these patches as quickly as possible. The longer equipment goes unpatched, the higher the probability an attacker will scan and find a publicly available vulnerability. The infamous Equifax breach where 143 million users lost data to an attacker was due to an unpatched server. The Apache Struts application used on public-facing Equifax web servers had a vulnerability patch released in March 2017, but attacker scans found the unpatched equipment and exploited it in September 2017. Failure to properly patch the system was the primary cause in one of the biggest data breaches of the decade.

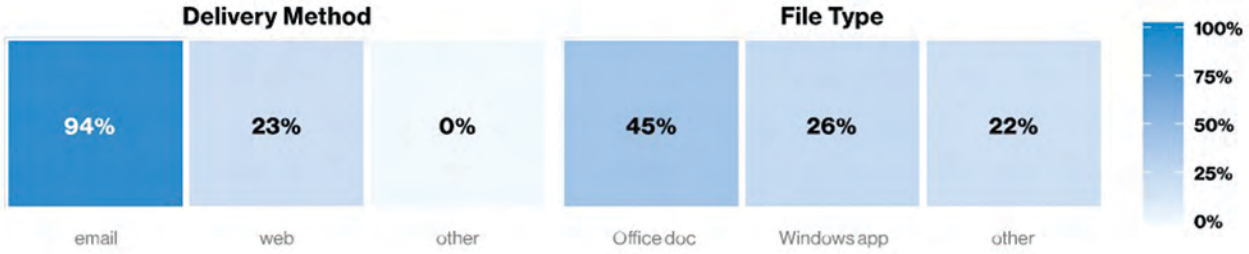
2. Human Error and Phishing

In Verizon's 2019 Data Breach Investigations Report (DBIR), "hacking" was a prominent vector leading to data breaches. "Hacking" is a broad category, but the two largest subcategories were "web application" and "stolen credentials." Vulnerabilities in frontend web applications resulted from unpatched software described above, but the second cause was stolen credentials from phishing campaigns.

Phishing campaigns include the use of email, SMS messages, and voice calls. The quality of user education has an impact on human error and data loss, but employees come and go every year with new ones less likely to detect an attack. It's clear that phishing and human error should be the biggest concern for organizations fearful of large data breaches.

3. Malware Installation

Malware is often coupled with email phishing campaigns, but this only represents a portion of what it can do when introduced to an organization's network. Ransomware is still an issue for organizations, but its popularity has dropped. According to Verizon's DBIR mentioned above, backdoors, control and command (C2) applications, email attachments, and keyloggers are the current tools of the hacking trade. Every one of these malware vectors can lead to stolen credentials and data breaches.



Source : Verizon DBIR – Common Delivery Methods and File Types in Malware Attacks

The most common malware attack incorporates email attacks with attached Office documents. Once downloaded, users opening a malicious document are prompted to run macros (unless Office is configured to always run macros without notifications). These macros download additional malware that can include backdoors, ransomware, keyloggers, C2 applications and numerous others.

4. Insider Threats

Insider threats can be malicious or innocent naïve users opening malicious attachments. Both are equally dangerous to cybersecurity posture, but malicious insiders are a different flavor than the standard targeted naive users. Malicious insiders could be a part of corporate espionage where competitors pay a targeted organization's employees for sensitive trade secrets. They can also be disgruntled employees focused on doing harm to their employer.

Data breaches often have monetary motives, and stolen user data could bank a malicious insider many thousands (potentially millions with enough quality stolen records) of dollars. Experian researched how much user data is worth, and the most valuable is medical data that can fetch the seller up to $1000 per record.

5. Physical Theft of a Device

Employees that bring their own devices make it easier for them to work from home and an office but storing corporate data on the device increases the attack surface of the organization. Poorly configured devices or ones with little-to-no cybersecurity defenses open the organization up to potential data loss after physical theft.

Whether it's a smartphone, laptop or tablet, an organization without a bring-your-own-device (BYOD) policy is much more vulnerable to a data breach. Not only could the device be stolen and data extracted, but users connecting devices to public Wi-Fi without the right configurations and cybersecurity defenses could open data to anyone connected to the hotspot.

Exploring the Dangers of Human Errors to Data Security

What makes human errors so frustrating for IT staff is that users aren't naturally qualified to detect ongoing attacks, and they create the weakest link in the cybersecurity chain. Even worse, according to Verizon DBIR, the average time it takes for a compromise is 140 seconds, but it takes months to discover the breach and several more days to contain it.

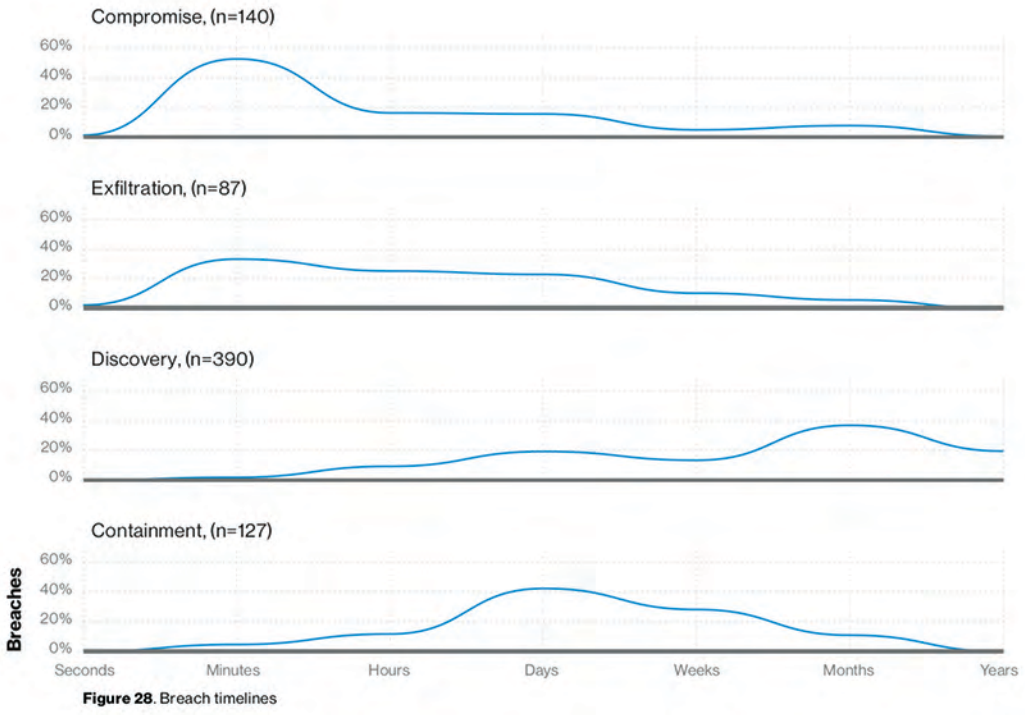


Figure 28. Breach timelines

Source : Verizon DBIR – Common Delivery Methods and File Types in Malware Attacks

Organizations should train users to detect attacks but even trained IT staff fall for common social engineering and phishing attacks. Once a user gets tricked into downloading malicious files, malware such as ransomware quickly scans the network and can be devastating to data integrity. Take one of the fastest-spreading, destructive malware attacks of the 2010 decade – WannaCry. Once executed, the malware leveraged Windows Server Message Block (SMB) to scan the network for open directories where it encrypted corporate data and held it ransom. WannaCry was a global cyber-attack that affected 200,000 computers across 150 countries and is estimated to have cost billions in containment and recovery costs. According to Kaspersky, human factors played a major role in the success of the WannaCry malware epidemic.

IT staff share some of the blame for successful phishing campaigns. Privilege escalation and abuse enable malware to infest infrastructure from what should be low-privileged user actions. Users with one set of permissions that transfer to new departments where additional permissions are given without revoking old permissions. In other cases, users leave the organization where access to obscure systems is forgotten. Privilege aggregation isn't uncommon where users continue to have additional permissions assigned without unneeded access revoked. The result is that a user who has been with the company for a while could have the equivalent of administrative access on the network, making the user the perfect target in a spear-phishing attack.

TitanHQ™

2020 Guide to Data Breach Prevention

Corporate and Personal Email Play a Major Part in Cyber Breaches

Email is one of the most insecure forms of Internet communication, but it's convenient and ingrained into any business. There are three main types of cybersecurity concerns with business and personal email:

- Phishing attacks including spear-phishing where users are tricked into opening malicious files or divulging private data such as authentication credentials.
- Hacked accounts due to stolen credentials.
- Stolen devices with corporate email and poor cybersecurity controls.

Although personal and corporate email should be separated, it's not uncommon for users to use a personal email with corporate data. For instance, a user who decides to work from home could forward messages to personal email. If this user's personal email is hacked, data disclosure could be an issue without the organization having any control over the third-party system.

Cyber-attackers are well aware of the loose rules and operating procedures surrounding email, which makes it an easy target. Number one and two listed above are primary issues for organizations that can be controlled. The third issue can be controlled as well by implementing strict rules around the transfer of sensitive data. Insider threats are a real concern for IT but just like phishing and hacking, the right cyber-defenses on email systems can drastically reduce the risk of threats.

Hacked email accounts are often the result of phishing, so the first two issues go hand-in-hand, and they lead to severe breaches where millions of records can be lost to attackers. When users think of hacked accounts, they think of an attacker purposely targeting their data. In fact, many of today's attacks are scripted and untargeted. Thousands of phishing emails are sent where attackers just find the needle-in-the-haystack users that could give them access to sensitive data. In addition, attackers build long lists of stolen credentials and then sell them online where hundreds of other attackers can hack away at vulnerable accounts.

In January 2019, 800 million login credentials were uploaded to darknet markets and hacking forums. The disclosed credentials were the result of phishing attacks and data breaches accumulated until attackers were able to share and sell sensitive data. This event is just one of the numerous data breaches that involve phishing for credentials. After a user discloses network credentials, attackers log the information in a database with other phished credentials. Once sold, any user can perform a search for an account name or email and find the disclosed password. Attackers take a database of credentials and use scripts to attempt authentication. If successful, the compromised account can be used to install malware on the network, eavesdrop on corporate data, set up additional backdoors in case the compromise is detected, and even install malware that will give remote control of the local device.

It's not uncommon for users to use the same password across multiple platforms, so a successful attack on personal email could mean a breach on business email. Two-factor can help mitigate and deter the average attacker, but the SS7 protocol responsible for transferring a random two-factor PIN to a user's smartphone was compromised and isn't a difficult hurdle to overcome for a savvier bad actor.Expiring passwords and forcing users to change them after a given timeframe (e.g. 30 days) reduce the risk of disclosed credentials, but users will often use a similar or the same password multiple times. Network access rules overcome this hurdle by forcing users to change passwords to a unique value, but attackers still have an open window where a user account is vulnerable to unauthorized access.

TitanHQ™

2020 Guide to Data Breach Prevention

The Cost of a Data Breach Could Reach $150 Million Annually in 2020

Losing sensitive data to an attacker is just the start of a long process that includes forensic investigations to find the perpetrator (if possible), notifying customers that their data was disclosed, legal ramifications from lawsuits, brand damage and loss of trust leading to possible stock price plummeting and client abandonment, and numerous other factors that can affect the business for years afterward.

As noted previously, IBM reported in 2019 that the average cost of a data breach was $3.92 million, but recent research by Juniper Research indicates that 2020 is projected to see exponential growth in annual data breach costs. It's estimated that the cost of a data breach this year could reach $150 million annually with the potential to be over $2 trillion globally.

The rise in costs stems from hacking turning into a professional business and the darknet monetary potential for a successful attacker, depending on the type of data and the number of records exfiltrated. The popularity of IoT provides attackers with new opportunities and vectors. Most consumers and organizations are connected to the cloud, which opens the risk to threats from the public Internet.

Another issue contributing to high costs is the extensive amount of time it takes to identify a breach. After months of unauthorized access, an attacker can exfiltrate potentially terabytes of data without tripping intrusion detection sensors. Regulatory standards such as PCI-DSS or HIPAA have high fines for organizations found to have poor cybersecurity that doesn't follow specific rules. For instance, the average cost of a healthcare data breach is $429 per record putting a lot of responsibility on healthcare organizations to protect data at all costs.

Data breach cost isn't immediately realized and finished after investigation and containment. Residual costs persist for years later for some organizations. Target, whose missteps led to one of the largest credit card number breaches in 2013, settled lawsuits in 47 states for $18.5 million four years after their cybersecurity incident. From March 2015 to May 2017, Target paid millions in lawsuits, a settlement with Mastercard and Visa, and costs paid to credit unions and banks. Overall, Target paid $300 million in costs associated with the data breach, but $153 million of these costs were legal fees.

Data Breach Prevention Using Email Cybersecurity

Of the five aforementioned data breach causes, three of them can be linked to email misuse. That's 3/5 linked to email misuse! Whether it's an insider threat using email to send data to a third-party or a naïve user falling victim to a phishing attack, email monitoring, filtering and cybersecurity tools are necessary for cybersecurity and data protection. But even high-level executives and high-privileged users occasionally fall for phishing scams.

Training and educating users are the primary methods for most organizations. All users should be trained to identify phishing even low-privileged users. Privilege escalation attacks can happen should an attacker gain access to these user accounts. The most effective way to prevent data breaches from phishing and other email exploits are to proactively identify attacks, filter them, and quarantine suspicious messages.

TitanHQ

2020 Guide to Data Breach Prevention

Data Breach Prevention Using Email Cybersecurity

Email cybersecurity isn't new technology, but better artificial intelligence (AI) and sophistication have been developed to better detect malicious incoming messages. The Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol also eliminates spoofed sender addresses, which is a common component of a phishing attack. Using DMARC with AI filters reduces the chance an email message reaches a targeted user's inbox. Add training to the mix, and any false negatives will be ineffective.Unpatched software and firmware were prominent reasons for cyber breaches in the last few years, and the only way to avoid this exploit is to keep a frequent update schedule for all infrastructure. Vendors always announce new patches and updates and the vulnerabilities fixed by installing the latest firmware versions.

Organizations that allow users to take home corporate devices should take precautions should they ever get stolen. Encrypting the local drive eliminates the potential of stealing data from the device, but other options include tracking and remote data wiping applications. The device may never be found, but wiping the data saves the organization from data breaches. In addition to physical device cybersecurity, the use of a VPN will help prevent eavesdropping and data theft when employees use public Wi-Fi. VPN services will encrypt all data that passes over the Wi-Fi hotspot, so poorly configured hotspot routers or attackers eavesdropping on data will not be possible.

Cybersecurity Predictions to Watch in 2020

No one can tell you what will happen in the next decade, but the fact is that the cybersecurity landscape is much more advanced than it was in 2010. Attackers have more technology at their disposal, and the cloud has introduced benefits with the disadvantage of additional risk and threats to organizations. To deal with an always evolving cybersecurity landscape, being proactive will avoid the trending exploits and attacks used to evade outdated equipment. Here are a few trends to follow.

Credential stuffing will continue to plague organizations. Credential stuffing is the term given to using lists of credentials online to find vulnerable accounts. Organizations will need better intrusion detection and implement multi-factor authentication to help stop attackers. Phishing will continue to be a favorite for attackers. Between malware installations and credential theft potential, attackers can launch thousands of emails at one time to targeted users. It only takes one user to send the right information for a successful breach. Email filters and cybersecurity to detect these attacks will greatly reduce phishing's success for the attacker.

Ransomware will be the best profit for attackers. Organizations must choose between backups and paying the ransom fees. For some organizations, the only option will be to pay the attacker if no backups exist. Windows 7 users will be a target. Windows 7 "end of life" was January 14, 2020, which means that Microsoft will no longer be patching for vulnerabilities. Users still on Windows 7 machines put themselves at risk and will be vulnerable. Attackers will use AI and machine learning (ML) to their advantage. AI and ML can be used for good, but attackers can also use it to identify potential vulnerabilities. AI will be mainstream for most organizations but attackers will also leverage the technology's advantage.