Data Breaches/CyberThreats Faced by Small Businesses and How Threat Intelligence can Help

By Leonard Melnik

Data Breaches/CyberThreats Faced by Small Businesses and How Threat Intelligence can Help

Introduction

Cyber threats are faced by both individuals and corporations. However sometimes that line gets blurred and Small Businesses do not consider themselves at risk. That could not be further from the truth, over 43% of cyber attacks target small businesses ("2021 SMB Data Breach Statistics"). Meanwhile over 70% are unprepared to deal with such an attack. In this paper I seek to present the reasons why Small Businesses should prioritize their Cyber and Data security and how they could utilize Threat Intelligence to mitigate the most likely attacks.

With the current political/cyber climate CISA has warned "Every organization - large and small" to be prepared to respond to disruptive cyber incidents.

What is a Small Business

While different individuals may have unique opinions on what defines something as a "small business" , the official government census defines a small business by a revenue range of $1 million to $40 million and having an employee count of less than 1,500 (Hait). The census has these definitions because it allows them to capture 50% of the revenue of all the firms in the industry. So, anything with less than 1,500 employees is considered a small business.

What is Threat Intelligence

Threat Intelligence is the continuous process of planning, collecting, processing, analyzing, and dispersing information that poses a threat to systems and applications (as well as individuals). Threat Intelligence helps understand the motives, targets, and behaviors of threat actors (person or group that take action to cause harm). Companies or individuals that utilize threat intelligence are enabled to take quicker and more accurate decisions even before they are attacked.

There are various types of Threat Intelligence tools, although most are geared towards enterprise customers (not small businesses). Typically they aggregate and analyze large amounts of data from sources such as the Darknet, Social Media, and various others. Threat Intelligence empowers organizations to be proactive instead of reactive.

What is a Data Breach

A data breach occurs when any data is exposed to an unauthorized source, including (and most importantly) sensitive and confidential data. There are many threats that can cause a data breach, some intentional and some not. On occasion it has been known for insiders to accidentally expose information (due to a mistake or lack of knowledge), other times it is malicious with intent from an insider or outsider.

While these breaches can vary in cost, the average cost of a data breach was 4.35 million USD (IBM) and in 60% of organizations, the breaches led to the cost being passed onto the customers. These numbers do vary between reports, as, according to Symantec, the average cost of a cyberattack is $188,242 (but this figure does not include productivity loss, trust loss, and business loss).

On average, it took 277 days to identify and contain a data breach (IBM). This number has been consistent over the last 7 years. Logically, a shorter data breach lifecycle is associated with lower costs, as the company is not restricted in productivity for more days and can resume its regular operations sooner, as well as the hackers having less time to crawl through the system. And while the average duration of a life cycle has not increased, the cost has.

The effect that data breaches have on smaller businesses is devastating. 60% of small to midsize businesses who suffer a hack will go out of business within 6 months (Galvin et al.). A hint as to why small businesses may be targeted more is because, while large businesses hold data on a lot of customers, small businesses typically hold credit card numbers, photos of ID's, and other things that are very valuable to hackers. Not to mention SMB (small

Data Breaches/CyberThreats Faced by Small Businesses and How Threat Intelligence can Help

businesses) often lack proper security measures and their employees are not as trained.

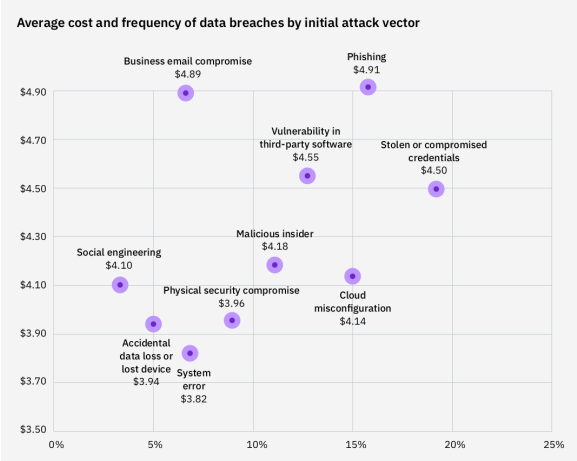


Figure 11: Measured in USD millions

Source IBM Cost of Data Breach Full Report 2022

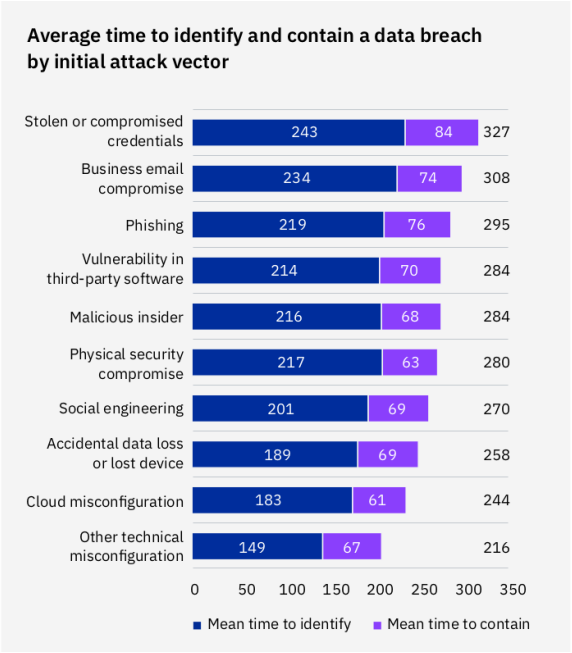
Attack Vectors and What They Indicate

The most expensive initial attack vector (that resulted in a data breach) was **Phishing**, which is the act of sending fake emails or messages pretending to be a reputable or legitimate source. Employees are being fooled or manipulated. This indicates:

- Poor security systems to detect and flag external emails/communications.
- Lack of awareness of phishing examples
- Little verification and/or open communication between employees

Phishing attacks often rely on scare tactics and urge the victims to respond quickly. When in this state of urgency, an individual may not recognize a fake. However if they were to discuss it with a team member or friend (even if it may be hard to share), then there is a higher chance the fake will be recognized.

Just to be clear, I do not classify an email being sent by a legitimate compromised host as phishing, as the malicious actor has already bypassed authentication. In other words phishing is fake emails being sent from fake sources.



Source IBM Cost of Data Breach Full Report 2022

The most frequent successful attack vector was **stolen or compromised credentials**.[1] Which was also the attack vector that took the longest to both identify and contain. This occurs when employee/critical accounts were leaked in other hacks/cybersecurity incidents. This is usually not directly the fault of the company, since the third party company that got hacked is the one that lost the critical data. However it is still the Small Businesses responsibility to change any credentials that have been compromised (whether by their own, or a third party's, hand). Companies such as DEHASHED boast a catalog of 14.5 billion compromised credentials and personally identifiable information.

Cloud Misconfiguration was the third most common attack vector but was the 6th most expensive. It often occurs when proper permissions are not set/and or proper testing is not done to ensure security. While this is also the fault of the business that suffers the breach, the software used should come secure by default, as one line wrong in the

[1] **Stolen or compromised credentials were also the second most common threat that faced small businesses according to Verizon's DBIR Report**

configuration can invalidate the whole authentication process.

This attack vector was brought up in a warning by CISA that stated “If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA’s guidance.” Due to lack of training and resources, it is likely that small businesses are more likely to make mistakes regarding Cloud Misconfigurations.

How Threat Intelligence Can Help

According to joint research between FINRA, BBB, and Stanford Center of Longevity, “Prior knowledge of fraud helps decrease the chances of victimization.” If employees and users are more educated regarding the risks, there is a lower chance that they will fall victim. This is especially true in regards to phishing where if the employees can see examples, then they will be able to more accurately recognize them and not fall victim when automated filtering fails.

In 2022 19% of breaches occurred because of a compromise at a business partner (IBM). All of the small businesses that I have spoken to all did not understand the value proposition of Threat Intelligence since often the company who experienced the breach already knows it has been breached, so what's the point? News of breaches reach the clearweb and news much later than Threat Intelligence software, and if a company can find out its partner or service provider was breached. They can take action and potentially save themselves from a breach.

Regarding Stolen or Compromised Credentials, Threat Intelligence benefits in two parts. The first part is detecting when a business has been hacked. If Business A uses the services of Business B, and Business A’s Threat Intelligence software has just notified them that Business B has been breached. Business A can take actions such as changing passwords that were used, actively monitoring emails and phone numbers provided to Business B, as well as possibly take their needs to a different provider who is not as likely to get hacked.

The second part where Threat Intelligence addresses the credential issue is with the actual credentials themselves. To be notified a company was breached is one thing, but to see the information that was leaked/be notified if your data has appeared in a leak is another. As discussed earlier, stolen or compromised credentials take the longest to identify and contain out of all other initial attack vectors. Certain Threat Intelligence and data aggregator services can collect all the compromised accounts and notify you if there is a match, additionally they can prevent your users/employees from using credentials that have been exposed in a hack which will prevent any future damage from those breaches.

A lot of the database breaches contain hashed passwords, which are just the passwords mashed up in a way that is irreversible, but if it is mashed in the same way (with the same algorithm) then the hashes will match. While this means Threat Intelligence cannot get the original password (directly), they can hash any password you attempt to use and compare that to their records to see if there is a match.

Not only can there be security flaws in companies, but there can also be security flaws in software. CVE’s (Common Vulnerabilities and Exposures) are publicly disclosed in an effort to make security more transparent and are a critical part of Threat Intelligence. By keeping up to date on CVE’s you can be alerted when software or system you are utilizing have weaknesses that can be exploited as well as testing them against your systems to ensure/test if the exposures have been patched.

Threat Intelligence for individuals

While this paper is regarding businesses, I wanted to quickly go over the benefits of individuals utilizing threat intelligence. Since the weakest link of any security system are the humans, it makes sense that

Data Breaches/CyberThreats Faced by Small Businesses and How Threat Intelligence can Help

Threat Intelligence should also help them. Now as I will discuss later, Threat Intelligence is "Intelligence". The more you know the better actions you will take, but it is up to the individual to seek out the knowledge (or Threat Intelligence). Just as the average individual watches sports and keeps up with war efforts/news, I propose that individuals should also keep up to date with cybersecurity news and threats. The most vulnerable in our society are often manipulated by phishing and scams, by making this education a standard we can help protect and save people from risky situations.

This is a topic that could and hopefully will warrant its own paper, but it is something I wanted to briefly mention.

What Can't Threat Intelligence Do

Threat Intelligence is so, it is Intelligence. It must be utilized properly, but in the end it is the actions of the "Intelligence" beholder that will influence whether a breach or incident occurs. As it is well known in security and in life, nothing is 100%. But that should not stop us from taking actions to get as close to that as possible.

Proper policies and training should be put into place. Secure and non spoofable MFA or 2FA should be used, and employees should be empowered and enabled in cyber and general security.

Conclusion

Threat Intelligence is a very powerful tool that should be utilized by both small and large businesses, not only does it help by educating employees on examples of real phishing and other attacks, it also keeps the company safe by monitoring their assets to ensure they have not been compromised. As small businesses tend to store data that cybercriminals want, and typically have less means of defending them, they are increasingly targeted with various cyberattacks. Cybersecurity is no longer just a priority for large corporations, but now is for everyone.

Works Cited

Chen, Patrick. "Report: Cyberattacks Affected 42% of Small Businesses in Past Year." AdvisorSmith, AdvisorSmith, 8 November 2021, https://advisorsmith.com/data/small-business-cybersecurity-statistics/. Accessed 17 December 2022.

CISA. "CISA Cybersecurity Awareness Program Small Business Resources." CISA, CISA, https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-small-business-resources. Accessed 17 December 2022.

CISA. "Shields Up." CISA, https://www.cisa.gov/shields-up. Accessed 17 December 2022.

CISA. "Stop Ransomware." CISA, https://www.cisa.gov/stopransomware. Accessed 17 December 2022.

Galvin, Joe, et al. "60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself." Inc. Magazine, 7 May 2018, https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html. Accessed 17 December 2022.

Hait, Andrew W. "What is a Small Business?" Census Bureau, Census Bureau, 19 January 2021, https://www.census.gov/library/stories/2021/01/what-is-a-small-business.html. Accessed 17 December 2022.

IBM. "Cost of a data breach 2022." IBM, 2022, https://www.ibm.com/reports/data-breach. Accessed 17 December 2022.

Kotsias, James, et al. "Adopting and integrating cyber-threat intelligence in a commercial organisation." European Journal of Information Systems, 2020, https://doi.org/10.1080/0960085X.2022.2088414. Accessed 17 December 2022.

SBA. "Strengthen your cybersecurity." Small Business Administration,

https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity. Accessed 17 December 2022.

"2021 SMB Data Breach Statistics." Verizon, 2021, https://www.verizon.com/business/resources/reports/dbir/2021/smb-data-breaches-deep-dive/. Accessed 17 December 2022.

Verizon. "2022 Data Breach Investigations Report." Verizon, https://www.verizon.com/business/resources/reports/dbir/. Accessed 17 December 2022.