Predictive Analytics Group®

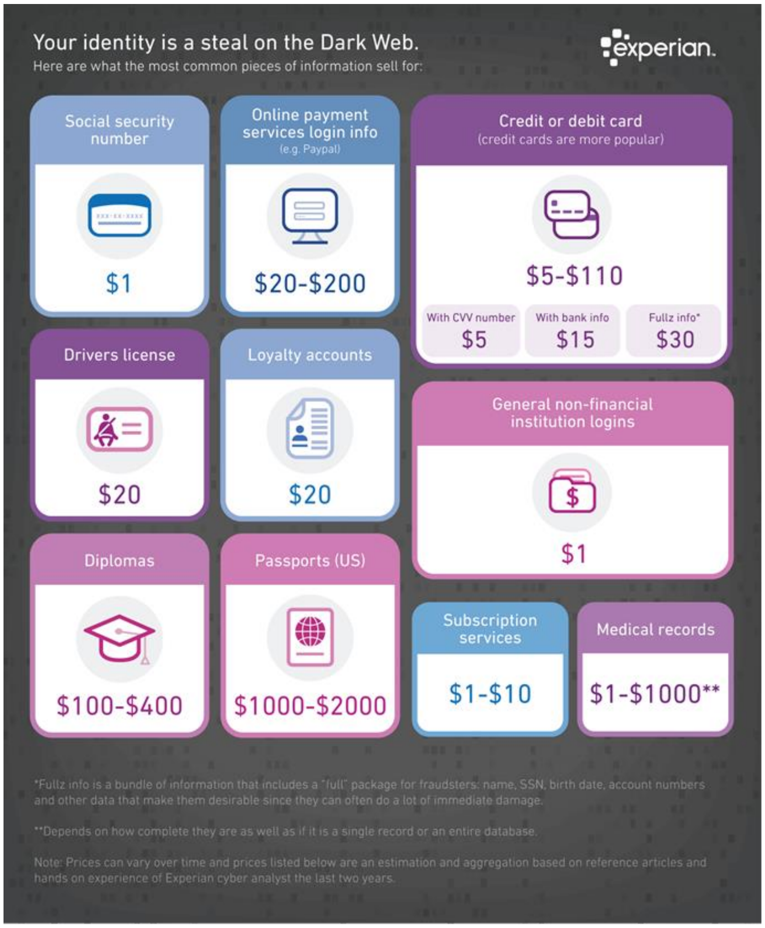
Analyze Tomorrow Today

Beating Back the Beast:

Cybersecurity in the Financial World

You read all the IT reports, you follow their recommendations, and you pay attention when they inform you of risks and problems. Many of your associates or those you know do the same. Yet somehow, you still hear about breaches in businesses everywhere, including your personal network.

The reality of the current climate is that it's not IF but WHEN with data breaches. Data breaches are an evolving, everlasting problem for all businesses. Targets for data breaches can extend from the "mom and pop" corner stores to every Fortune 500 company. While you are growing your business, hackers are growing theirs.   Equifax or not, your data has a big price tag.


Your identity is a steal on the Dark Web.
Here are what the most common pieces of information sell for:
experian.
Social security number
$1
Online payment services login info (e.g. Paypal)
$20-$200
Credit or debit card (credit cards are more popular)
$5-$110
With CVV number $5
With bank info $15
Fullz info* $30
Drivers license
$20
Loyalty accounts
$20
General non-financial institution logins
$1
Diplomas
$100-$400
Passports (US)
$1000-$2000
Subscription services
$1-$10
Medical records
$1-$1000**

*Fullz info is a bundle of information that includes a "full" package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage.

**Depends on how complete they are as well as if it is a single record or an entire database.

Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.

Figure 1 (Experian, 2017)

The Cybersecurity Beast

Let's take a quick look at some of the biggest financial breaches.

Major Financial Breaches of the 2010s

Company	Year	Number of people affected	Information Compromised	Cost (in USD)
Equifax[1]	2017	143 million	SSNs, names, birth dates, contacts*, etc.	1.4 Billion
JPMorgan Chase[2]	2014	76 million households	Contacts*, addresses, names, etc.	Undisclosed
Capital One[3]	2019	106 million	SSNs, account numbers, names, birth dates, contacts, reported income	Predicted 100 to 150 million

**Contacts includes information like phone numbers, email, etc.*

[1] *(Fruhlinger, 2019)*

[2] *(Silver-Greenberg, Goldstein, & Perlroth, 2015)*

[3] *(McLean, 2019)*

We can see that in recent years the situation has not improved regarding breaches ; they continue to carry high price tags. Not every company is as large as Equifax, and many companies don't have nearly as large of a budget. Yet small businesses have as much responsibility to protect their customers' SSNs, names, birth dates, account numbers, and other highly sensitive data. Smaller businesses are just as much of a target as large ones but they have significantly less resources. This challenge compares well to the Greek story of Sisyphus.

Sisyphus, a character in Greek mythology, managed to trick and deceive the gods multiple times and to punish him, Zeus had Sisyphus roll a massive stone up a hill every day. And every time he nearly reached the top of the hill, the massive stone would roll right back down to the bottom.

With cybersecurity, we can end up feeling like Sisyphus, stuck forcing our way uphill but never catching up. Every day, another breach is announced on the news somewhere in the country. Somehow, despite this acute awareness, many companies haven't been able to beat back the cybersecurity beast.

(Titian, 1548-1549)

A high level bank officer recently commented that "cyber security is discussed everyday with top management, it is the most pressing concern [they] have. No longer is the threat of a branch holdup the concern for loss, [they] have that covered, [their systems] get attacked countless times every day."

For financial institutions across the U.S., cybersecurity remains the stone they can't quite get up the hill. In today's cyber world anyone may be a target, and many are. According to Verizon's report, 43% of breaches target small businesses (2019, p. 5). This is particularly concerning for the financial industry, which has such valuable information to safeguard like SSNs, names, birth dates, account numbers, making it an especially tasty target. This reality isn't anything new to anyone. What is the cybersecurity beast like now, and how do we beat it back?

The Current Climate

The current state of the cyber world focuses heavily around moments when security falters; in other words, breaches. The average cost of a breach in the U.S. in 2019 was 8.19 million dollars (Verizon, 2019), with the average financial industry costs second only to healthcare. Money isn't the only factor, as information is as valuable an asset as money itself and losing it can have lasting ramifications. Breaches also harm customer relationships. A global study conducted by Gemalto, a cybersecurity company, reported 59% of customers said they would move to another financial institution if they were breached (2017). According to the Verizon report, lost business is the largest cost factor involved in breaches for 2019 (2019).

Executive Summary

Cybersecurity in the financial industry is tenuous at best in a climate of increasing attacks. Everyone in the financial industry must be familiar with the information and tools discussed here.

- Cybersecurity is a difficult challenge, especially for smaller financial institutions, but everyone is a target for attacks.
- Cyber attacks are rising in frequency and cost a lot for the target. The average cost of a breach in the U.S. in 2019 was 8.19 million (Verizon, 2019).
- Currently some tools are already used like anti-malware software, encryption, system backups, and strong passwords.
- Some newer, effective tools worth consideration include multi-factor authentication, data viewing management, no-trust environments, and incident response teams.
- Institutions must prepare a plan for when breaches occur and regularly practice the plan with all employees.
- In the future, businesses must be mindful of the security concerns involved with Cloud technology and the Internet of Things.

With these tools and a plan, financial institutions can gain ground on the fight to secure their data. Stay wary, stay safe, and we can manage the dangers of the cyber world.

Breaches don't just cost a business in the first year; only ~53% of costs occur in the first year for the financial industry (Verizon, 2019). This is a stark difference from the overall average of 67% of costs in the first year (Verizon, 2019). The financial industry can expect longer term costs from a breach.

Attacks grow more sophisticated and advanced as time goes on, and they aren't just from random individuals across the globe anymore. In the financial industry, 10% of breaches were attributed to national governments (Verizon, 2019, p. 41). Still, attacks are not the only source of a breach to consider as breaches from glitches and errors made up 49% of 2019 breaches (Verizon, 2019).

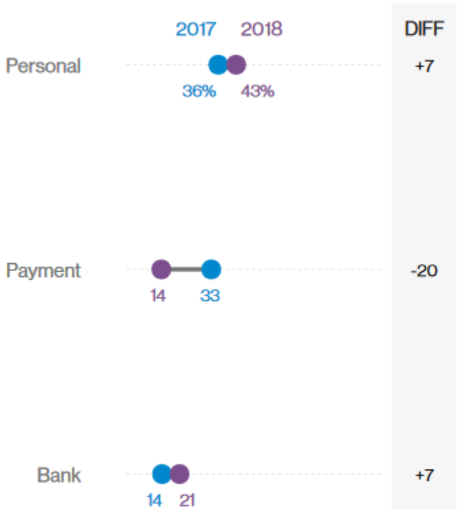


Figure 2 (Verizon, 2019, p. 42)

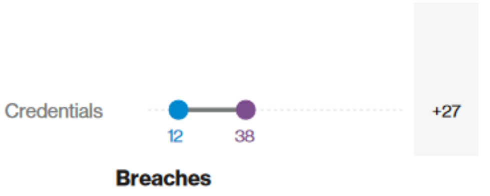


Figure 50. Select data varieties in Financial breaches over time
n=144 (2017), n=125 (2018)

In 2019, the chance of a breach within two years was 29.6% for a company, about a third more likely than it was in 2016 (Verizon, 2019). Remember that this goes for businesses of many sizes, and no business is excluded from that. The financial industry appears to be the biggest target other than the healthcare industry. As a director in the financial industry, it's deadly to assume one is too small, or too secure. Today, it is apparent banks and credit unions must be more vigilant than ever in their cybersecurity.

The Classic Tools: What we've been using and why

In cybersecurity there are a few tools we've been using for years which continue to serve us well.

Antimalware Software: Software which serves to defend against and detect malware on a device. It may seek out and remove malware on a device and may also proactively help to block malicious software from installing or running.

Encryption: Techniques which transform data into a code unreadable for those who do not have the key to the code. This serves to protect data even if it is compromised as it will be indecipherable without the key.

System back-ups: Creating both physically and digitally a system which an organization can revert to should their primary system be ransomed or otherwise incapacitated.

Strong Password Policies: Strong passwords, ones with considerable length and various characters, are essential. It's also of great importance that passwords are not reused by employees as these passwords may have been compromised previously.

Future Tools: What haven't we been using, and why should we?

We've had a lot of incredibly useful tools at our disposal for years, but there are some recent tools which have come to light that may be of note.

Multi-factor authentication: Using more than just a username and password to verify a login, such as a text code to a mobile phone. Although this method is even now becoming outdated as perpetrators have recently been contacting employees to request the one-time password, a strong internal education program will help to keep employees vigilant and protect financial data. While not without its flaws, additional friction like this does help reduce stolen credential attacks. Such attacks were one of the most pervasive for the financial industry (Verizon, 2019, p. 42).

Data viewing management: Employees should not be able to view just anything, and measures should be in place to determine what each employee can and cannot view. Logs should be in place to track who sees what and employees should be aware they exist. Privilege abuse is still a major risk factor, particularly in the financial industry (Verizon, 2019 p. 43), with such a massive yet necessary amount of information.

No Trust environment: A recent trend in system design, no trust environments involve distrusting users in every part of a system. This means implementing further ‘gates’ requiring passwords or otherwise to continue. At no time should a user be assumed legitimate under this design. This serves to make infiltration more difficult, however it impacts ease of use. Despite that tradeoff, properly implemented, it can minimize the contamination from a breach.

Incident Response (IR) team: A team of individuals designated to head the effort in containing, analyzing, and ending a breach. This team should be determined in advance, design a comprehensive plan, and practice this plan regularly. See below for further information regarding IR teams.

Breaches: How do we prepare?

No matter how many layers of security or cybersecurity measures are in place, breaches are still a real possibility. While all preventative measures feasible should be taken, breaches are an unavoidable reality for any business. How can a business prepare for a breach?

Make a Plan

The first step to preparing for a breach is designing a plan. Every employee of the company, from top to bottom, should at least be familiar with the plan and should know exactly who to contact if a breach should be detected. Assess the need for third party assistance depending on the capability of a company's resources. A breach plan should contain the following:

1. **Pull the "fire alarm".** Everyone in a company should know the exact procedure to follow in order to alert the company a breach may be present.
2. **Plug the leak.** The IT team should drop any other priorities and stop the breach from worsening or continuing.
3. **Gather the IR team.** Make the marketing team aware the company will have to communicate with customers about the breach and handle the public fallout. Whoever is designated to communicate with government entities and regulators should begin this process.

4. **Determine the extent and cause of the breach.** Now it's time to determine what occurred during the breach and repair whatever problem started it. At this point the data forensics/IT team should be brought in to do so.
5. **Clean up.** Have the marketing team inform customers of the consequences of the breach. Be sure that all information regulators and government entities require has been communicated. At this point, it's time to inform the company as a whole.

Decide the IR Team

The second step to preparing for a breach is to determine who will be in the Incident Response team. This team should not only be composed of IT members, but should also include high level company members, marketing or company image experts, the CFO, and a data forensics team which may or may not be from a third party. The IT members serve an obvious role, but the other team members are just as important. The high level company members are necessary to serve as they usually manage, but to focus their energies in managing the breach. The marketing members should be present to help assuage the damage to customer relations and communicate with the customers as information arises. The CFO should be involved to assess the impact and plan for resulting costs. Finally, the data forensics team should be present to determine the events which led to and aftermath of a breach.

Practice the Plan

The final step is to practice this plan. In emergencies, everyone's responses need to be as attuned as possible. Members scrambling through a dusty manual will lead to oversights or mistakes. Communication here is the most essential part for executives to be familiar with for emergencies like breaches. Communication is the most essential part that may be forgotten for all members, which is the true goal of practice. Know who to call and when.

Practicing the plan may also evidence oversights or inefficiencies in the plan and provides the opportunity to find them before they cause significant impacts. Make amendments to the plan based on the results of practice.

While this may seem intimidating, the only defense against the grim reality of a breach is preparedness. Regardless of how robust a system's defenses may be, this preparation is essential. In this, IT and executives need to work together more seamlessly than they ever have.

The Future Climate: What should we be aware of?

Now that both past and present have been addressed, what about the future? While cybersecurity considerations and projections are highly dynamic, a few trends have evidenced themselves.

The Cloud

The first is the Cloud. The Cloud is a service where a service provider provides another company the physical components of their digital system. It's like renting tools from a company, except that these tools are for digital purposes. It's growing massively in popularity with businesses across the globe in just a few years. It's a convenient and cost effective service, so this is not surprising. However, there are major security concerns involved with this service.

The first is more apparent, which is that using The Cloud means an institution depends on the company providing them the service. If their servers crash, or their systems are infiltrated, you will suffer with them. Although Cloud providers are large and robust, we all remember how "too big to fail" can be a pitfall. These companies are not required to be very transparent about their practices, and they likely won't be. Even if they are, how can you trust what they claim? Cloud service providers are not necessarily 'bad', but they do warrant some suspicion and caution.

The second problem is less apparent, which is its ease of use. Cloud services are designed for ease of use, not for security, and so the default settings are usually dangerous for companies to utilize (Trend Micro, 2018). A common misconception about breaches is that they're always malicious, but errors account for 21% of breaches according to the Verizon Data Breach Investigation Report (2019, p. 22). These default settings are a known pitfall which security companies warn to avoid (Trend Micro, 2018).

It is the responsibility of a financial institution to determine what should reside in the Cloud. Further, the appropriate processes and controls must be in place and an institution must assure these measures are operating effectively.

The Internet of Things (IoT)

The other trend which grows in magnitude and difficulty by the day is the Internet of Things. Internet of Things refers to the systems of today where all kinds of devices are interconnected by the Internet in the hands of all kinds of people. This leads to further convenience, but the tradeoff is a degree of cybersecurity.

At any time, an employee can take out their phone and take a picture of their computer screen. Around sensitive data, this can be catastrophic. No matter how well defended a system is, it can't prevent employees from using their devices improperly and endangering data. The only exception to this are total ban areas where no devices, pencils, paper, etc. are ever allowed.

For example, say an employee erroneously sends an infected email to a third party associate. This associate doesn't follow your rules, and the infected email compromises their system. Their system then contaminates yours, and suddenly you have a compromised system. Both your third party didn't protect themselves effectively and you did not isolate yourself enough. It's as if a virtual zombie apocalypse plague is everywhere, and you have no idea who has contracted it. You need to survive but protect yourself from everyone since anyone could be infected.

Unfortunately, this applies to your employees, who may also be infected with zombie apocalypse plague on their personal devices. If their devices are connected to your system or even present near your system (in the case of pictures of screens and so on), then they too could turn a part of your system into a zombie or otherwise compromise it.

Therefore, around extremely sensitive information, like young children or the elderly during a plague, extensive measures should be taken to protect the information from abuse or compromise. As our systems grow more connected and crowded, the 'zombie apocalypse plague' is all the more dangerous and likely, and thus we must be vigilant going forward.

Financial institutions must be wary of the dangers of this age of the Internet of Things. They must have and enforce policies regarding connected devices, both internal and external, and their use within the organization.

Conclusion

The past, present, and future in cybersecurity hold lessons for all of us to remember. We have the classic tools, and some newer to the stage which may be worth consideration. We know that the biggest risk is people, and the best thing to mitigate this risk is awareness and training. We know that breach plans are essential, IR teams must be determined, and the plan must be practiced. We're aware of the possible risks in the future with The Cloud and the Internet of Things. Cybersecurity is a rapidly changing field, and we must adapt with it to the best of our ability. Stay wary, stay safe, and we can beat back the beast.

FURTHER CONTACT PLACEHOLDER

Works Cited

Figure 1. Experian. (2017). [Graphic of the price of information like credit cards, names, etc. on the dark web, December 6, 2017.] Retrieved from https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

Figure 2. Verizon. (2019). [Graphic depicting the changes in trends of breach causes in the financial industry, 2018-2019.] Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Fruhlinger, J. (October 14, 2019). Equifax data breach FAQ: What happened, who was affected, what was the impact? Retrieved from https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Gemalto. (2017). [Graphic describing results of poll of customers on their feelings about breaches and how it would affect their choices.] *Data Breaches and Customer Loyalty*. Retrieved from https://safenet.gemalto.com/resources/data-protection/data-breaches-customer-loyalty-2017-infographic/

McLean, R. (July 30, 2019). A hacker gained access to 100 million Capital One credit card applications and accounts. Retrieved from https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

Silver-Greenberg, J., Goldstein, M., & Perlroth N. (October 2, 2015). JPMorgan Chase Hacking Affects 76 Million Households. Retrieved from https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

Titian. (1548-1549). Sisyphus [Painting]. Retrieved from https://en.wikipedia.org/wiki/Sisyphus#/media/File:Punishment_sisyph.jpg

Trend Micro. (2018). Misconfigured Cloud Services Pose High Security Risks for Organizations. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/-misconfigured-cloud-services-pose-high-security-risks-for-organizations

Verizon. (2019). Data Breach Investigation Report. Retrieved February 3, 2020, from https://enterprise.verizon.com/resources/reports/dbir/