M&A Cyber Security in the Financial Services Sector

SecureMerger®

Financial Services Cyber Security

Financial services professionals find a kindred spirit in meeting security professionals. They are both in the business of risk redistribution. Managing security risk is baked into the very core of financial services.

Financial service organizations strive to balance a reputation of stability against a healthy amount of innovation. Customers gravitate toward progress, so that is where the growth opportunities are. Yet nothing turns potential customers away more than the perception that the company does not have its situation under control. In short, security is the at the bedrock of financial services.

Organizations in this industry have found increasingly diverse ways of reaching consumers, which has likewise given criminals increasingly diverse ways of stealing from them. This draws regulators' attention from a number of directions (PCI DSS, GLBA, SOX, and GDPR to name a few), and requires that innovation prioritize information security. Standing as the guardians of online banking and payment card services, stock trading, sensitive personal information, and opportunities for tax or insurance fraud, it is no wonder that financial services is listed among the 16 critical infrastructure sectors which are vital to the United States' security.

What Criminals Want

From both an organizational and a consumer standpoint, the industry is attractive to criminals because this is where the money is. Analysis has shown the top three types of financial services data compromised[1] include:

- Personal data (Information useful for identity theft)
- Credentials
- Internal (Breaches of organizational information)

Attackers may use phishing, social engineering, or malware to steal credentials for accessing webmail, which leads them to organizational secrets. Recent years have seen a wide variety of sophisticated cyber attacks from organized international actors, specifically targeting the financial services industry with cyber espionage.

A 2019 global data risk report found that within the financial services industry, more than 20% of sensitive files (those containing personal or payment information that is subject to regulation) are accessible to every employee.[2] This is why credential theft is so attractive to criminals: it is a launching point for any number of thefts. Cyber attacks here are a means to an end.

1 2019 Verizon Data Breach Investigation Report
2 2019 Varonis Global Data Risk Report

How Criminals Get It

With friends like these, who needs enemies?

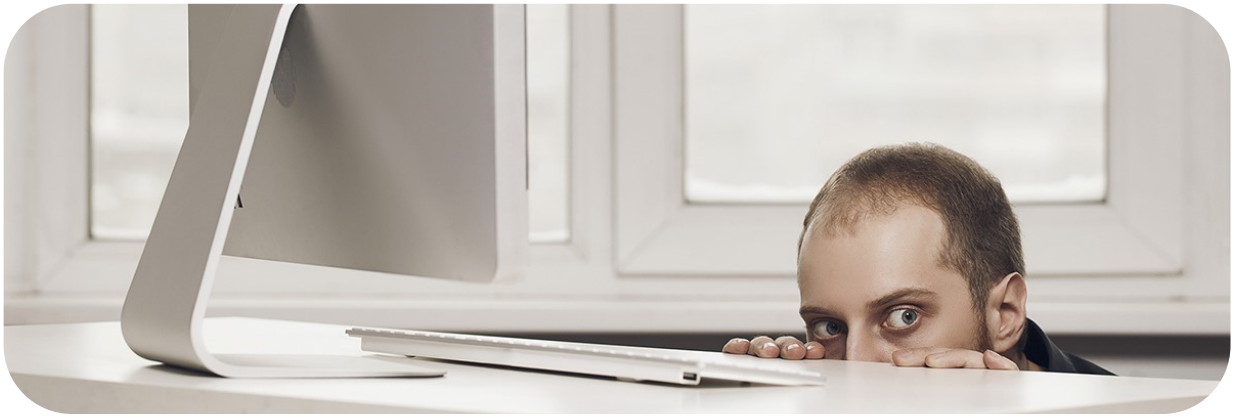
The financial services industry stands as an interesting case study on the placing of cyber security trust, and its consequences. It surveys as the industry which puts the highest degree of "complete" trust in its privileged employees and third-party vendors to safeguard sensitive information. Yet it is also the industry reporting the highest incidence of cyber breaches being attributed to employee access and third-party vendors.[3] It is easy to see the critical role that privileged users play in the security of this industry.

The top 3 patterns of cyber attack on this industry[1] include:

- Web application attacks
- Privilege misuse
- Miscellaneous errors (Misdelivery of data, etc.)

Web applications are a frequent target because they can include online banking, brokerage accounts, and web-based email. An attack on them may use any number of methods for fraudulently authenticating to an account, or may target code-level vulnerabilities that the developer either has not discovered, or has not patched.

Privilege misuse is a popular attack vector because it can encompass both the use of stolen credentials, and malicious insiders. Phishing and the use of stolen credentials in this industry far outstrip other attacks like hacking and malware. The use of stolen credentials is most often used on mail servers.[1] Obtaining credentialed access allows criminals to watch the internal workings of an organization long enough to impersonate a legitimate user. From inside the network criminals can launch any number of attacks, from collecting sensitive data to facilitating direct money transfers.



Within the financial services industry, the on-demand availability of sensitive information is critical to doing business. This has made ransomware a lucrative venture for cyber criminals in recent years. Even in spite of this, global insurance giant AIG reported that among cyber insurance claims, Business Email Compromise (BEC), which often includes fraudulent wire transfers, has become the primary cause of loss for cyber claims, and financial services is their second-hardest hit industry.[4] Criminals have found a weak spot in the industry.

The SEC issued an investigative report focusing on public companies falling victim to BEC, sometimes for tens of millions of dollars in losses.[5] As the SEC explained, "The frauds in some instances lasted months and often were detected only after intervention by law enforcement or other third parties."

3 2018 BeyondTrust Privileged Access Threat Report
4 2019 AIG Claims Intelligence Series: GDPR and Business Email Compromise Drive Greater Frequencies
5 SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls

To round out this discussion on attack vectors, the financial services sector has recently collected some dubious accolades, as highlighted in the Verizon 2018 Payment Security Report. The industry proved to be the

- *Worst at reducing systems' attack surface*
- *Worst at properly storing sensitive data*
- *Only industry getting worse at application security management*
- *Least compliant industry in using vulnerability scanning and penetration testing*

How Organizations In Transition Are Especially Vulnerable

M&A activity raises the stakes because technology and innovation are likely to be the motivating factors of many deals in this sector. A global PwC survey found that financial and FinTech executives expect startups to be the greatest source of industry disruption in the coming years, by a wide margin.[6]

All things being equal, financial services organizations face an unusually choppy outlook when in transition. Recent analysis shows this industry to have been the most cyber attacked industry for three years running. In 2018 it received 19% of all observed cyber attacks.[7] It is also three times as likely as other industries to suffer financial losses after a successful cyber attack.[8]

Firms may struggle in allocating the right resources to security, both in pre-transaction due diligence and in integrating and sustaining operations. The financial services industry's cost of cyber security compliance nearly doubled from 2011 to 2017.[9] When done in an inefficient manner, compliance activities can in fact detract from an overall security posture by becoming overly cumbersome and souring the organization's attitude toward legitimate security concerns.

One of the indirect threats that cyber attacks pose to the financial services industry is by way of customer churn. Customers' interaction with financial services firms occurs in close proximity to their money, so criminals have a shorter route to accessing that money by directing their attacks accordingly. Firms' image and goodwill are tainted by this experience, leading to the loss of clients and more difficulty in attracting new ones. For these reasons, this industry has the second highest churn rate (percentage of customers who leave after a data breach) at 6.1%, behind only healthcare. This stands as almost double the overall average of 3.4%. The consequence also gives the industry the second-highest average cost per record in a data breach, at $206.[10]

Finally, organizations in transition struggle more with detecting cyber attacks, because of the evolving state of "what normal looks like." In general, financial services organizations are only half as likely as other industries to see a disruption in their business processes after a successful cyber attack.[8] If you think that sounds like good news, read it again. It means cyber attacks can more easily go unnoticed in the financial services industry, because business processes continue as expected. How much harder these attacks may be to detect when the organization is transitioning both processes and people.

6 2017 PwC Global FinTech Report
7 2019 IBM X-Force Threat Intelligence Index
8 2018 KPMG Clarity on Cyber Security Report
9 2017 Ponemon Institute – The True Cost of Compliance with Data Protection Regulations
10 2018 Ponemon Institute – Cost of a Data Breach Study

What To Do About It

Organizations approaching an M&A activity, whether on the buy- or sell-side, can arm themselves against disruption by prioritizing a few strategies along the way.

Root out the usual suspects with cyber due diligence. We saw earlier that the financial services industry ranks as the worst in security essentials like reducing systems' attack surface, properly storing sensitive data, vulnerability scanning, and penetration testing. This provides a golden opportunity to identify these problems up front and make a plan to address them responsibly.

Prioritize security at the employee level. So much of what we have discussed above comes back to the exploitation of privileged users and accounts. An M&A integration plan that places an emphasis on employee training, the restriction of access and privileges around sensitive data, and smart monitoring of user activity is a good way to get the most dollar-for-dollar impact from cyber security spending in this industry.

Don't mistake compliance for security. Compliance activities have a narrower focus than the breadth of an organization's critical assets, and a myopic "checklist security" approach will probably not yield the most efficient of organizational strategies. Firms are better served by a big-picture approach to holistic security, which regards the wide variety of critical assets that impact the organization, and dollar-quantifies the risk that they represent to the bottom line.

If you're getting ready to sell, be proactive.
If you're getting ready to buy, ask questions.