FIVE CYBER SECURITY TRENDS FOR 2020

Julien Bonnay, Partner

The need for cybersecurity in the financial services industry has never been greater. Financial Institutions (FIs) have been and will continue to be the subject of cyberattacks by adversaries of all varieties. The old adage "why do you rob banks…. because that's where the money is" holds in this domain as well. In 2019, 86 percent[1] of breaches were financially motivated, and the records exposed in all breaches increased by 284 percent[2]. And if that's not enough for FIs to worry about, consider that the average cost of a breach as disclosed by public firms in 2019 was $116 million[3]. Given the magnitude of this issue, we have listed the top trends we've gleaned from our client work over the last year.

CRIME DOES PAY, ON THE DARK WEB, THAT IS.

Projections are that cybercrime will exceed $6 trillion annually by 2021 up from $3 trillion in 2015[4]. Probably the most significant factor driving this acceleration is the increasing efficiency of cybercriminals. The dark web has become a thriving black market where criminals of all means can gain the capabilities necessary to launch sophisticated cyberattacks. Gone are the days when attackers needed significant skills to launch an attack. In many ways, the dark web has commoditized attack tools while also providing a means of trading the spoils of an exploit. With Bitcoin and a Tor Browser, a would-be attacker, now has access to a plethora of malicious capabilities that include ransomware as a service, botnets for rent, and malware as a service, to name but a few. Given lowering barriers to entry and the financial payoff, expect cybercrime to continue rapid acceleration.

IT'S GOOD TO HAVE INTELLIGENCE.

As most FIs have realized, cyber threat intelligence is a critical component of a successful cyber program. Understanding adversary behavior and tendencies can help a firm anticipate and react quickly before or shortly after an attack. Many firms have instituted 'Cyber Fusion Centers' to facilitate this interaction. That said, significant challenges exist in operationalizing intelligence in a way that prioritizes activities for cyber defenders. A significant problem is the sheer volume of data available from multiple sources and the challenges associated with culling it into actionable intelligence to inform defensive processes such as attack surface reduction, detection logic creation and red team scenarios. Add to this the fact that security and orchestration technologies in existence today typically do not integrate well. Going forward, we expect continued emphasis on developing the next generation Cyber Fusion Center to extract value from cyber threat intelligence in a more streamlined and efficient manner.

1. Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexander Pinto, Suzanne Widup. "2020 Data Breach Investigations Report" (Verizon 2020)
2. Inga Goddijn, Executive Vice President,Risk Based Security. "Risk Based Security, 2019 Year End Report, Data Breach QuickView" (Risk Based Security 2020)
3. Audit Analytics. "Trends in Cybersecurity Breach Disclosures, May 2020"
4. Steve Morgan, Editor-in-Chief, Cybersecurity Ventures. "2019 Official Annual Cybercrime Report" (Herjavec Group, 2019)

THE CLOUD MAKES LIFE EASY.

Unfortunately, benefits can also accrue to those with nefarious intent – firms are moving to the cloud at an amazing clip and with good reason. Higher efficiencies, quicker speed to market and many enhanced capabilities drive up demand. Additionally, underlying cloud infrastructure can be more secure than legacy infrastructure thanks to additional attention paid by the cloud vendors as well as a consolidated and integrated approach. That said, there are pitfalls from a cybersecurity perspective. Chief among them is the need for comprehensive security solutions that incorporate the cloud as well as legacy infrastructure. Given the shortage of cloud security expertise and the lack of hybrid solutions that span cloud and legacy, companies are challenged to build in system-wide security. Also, due to the consolidation effects of the cloud, small errors in misconfiguration can have devastating consequences, as demonstrated by many recent breaches. Expect to see both increasing use and misuse of the cloud driving up the need for talent and integrated cloud security solutions.

YOU HAVE TO BE AGILE TO SURVIVE.

Today's customers are demanding the ability to transact fully and securely in the digital domain and competitors are offering new choices daily. FIs are realizing that keeping up in today's world of rapid digital transformation means adopting agile development. When done well, agile allows FIs to keep up with the rapid pace of technological change; however, building security into the process presents a whole new set of issues. Characteristics of agile development include small teams working quickly and iteratively, where you don't write requirements down, design and risk decisions are made just in time, and manual testing and compliance can't keep up with the speed of delivery. Clearly, our traditional waterfall approaches to building security can't keep up. To be successful, agile teams need a deeper understanding of security issues, willingness to adopt security practices, and must take increased responsibility for the security of their systems. In addition, security professionals need to work faster, more iteratively, and learn to view cyber risk and mitigations in more incremental terms. While all of these changes are possible, success often requires changing deep-rooted cultural drivers and incentives. It will not happen without a clear plan as well as an organizational commitment at all levels. Expect the transformation to secure agile development to remain a top issue for some time to come.

PEOPLE, ALL YOU NEED IS PEOPLE.

According to ISC^2, the number of unfilled cyber positions now stands at 4M professionals[5] world-wide. Add to this the fact that, according to the 2020 Verizon Data Breach report, nearly half all cyber incidents in financial services can be attributed to actions conducted by people. Clearly, we have a significant people issue. We fully expect our clients to continue to reach for assistance in finding qualified staff and training up the staff already on board.

5. ISC^2. "(ISC^2) Cybersecurity Workforce Study, 2019, Strategies for Building and Growing Strong Cybersecurity Teams." (ISC^2, 2019)

WHAT THE FUTURE HOLDS.

Going forward, it's clear that several factors are converging to increase cyber risk for FIs. Market forces continue to push FIs to rapid and comprehensive digital transformation, accelerating the use of technologies such as the cloud and agile and increasing exposure to the many inherent security issues. Moreover, the combination of an expanding talent gap and rapid growth of cyber-crime are trends that will continue for some time to come. FIs that invest in technologies and processes such as cyber fusion centers, secure cloud, secure agile and cyber talent development can greatly reduce cyber risk and significantly increase the probability that adversaries look elsewhere to exploit easier targets.

CAPCO

JN_2260