May 2019

Cyber threats to the financial industry

Data, geopolitics, and the growing cyberattack surface

Has the speed of information and transparency opened an unstoppable risk for the finance industry? Cyber threats continue to evolve and provide learning opportunities for risk managers to build defensible positions against them. We recently hosted a panel of cybersecurity experts who discussed how financial services organizations and their advisers can prepare themselves in the event of a cyberattack. As moderator Anne Joves, Associate General Counsel, National Futures Association, said: “Data is the crown jewel of a company in financial services.”

To better understand how to protect that crown jewel, the panel discussed the nature of cyber threats; information sharing and intelligence; risk mitigation; and how an organization can better prepare itself for when a cyber event happens.

Our panelists included LTG (Ret) Rhett Hernandez, former head of the US Army Cyber Command; Kevin Kirst, Principal in Cyber Security and Incident Response at Charles River Associates; William Rich, International Affairs Fellow at the Council on Foreign Relations; Tim Ryan, Managing Director at Sheltered Harbor; and N. MacDonnell (Don) Ulsch, Senior Consultant to CRA.

It’s going to get worse before it gets better – the threat landscape

The 2019 National Intelligence Strategy notes that cyber threats pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices.[1] Cybercrime is estimated to cost $6 trillion by 2021, up from $3 trillion in 2015.[2]

---

[1] Office of the Director of National Intelligence, “National Intelligence Strategy, 2019,” https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

[2] Cyber Security Ventures, “Cyberattacks are the fastest growing crime and predicted to cost the world $6 trillion annually by 2021,” news release, December 13, 2018, https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html.

With sophisticated attackers and increased automation, how do we keep up? Hernandez asked. A timely response to an incident is a great start; however, it's imperative to figure out how to prevent the attack in the first place. Persistent engagement and presence, including having people outside US boundaries to monitor activity and disrupt potential attacks are essential, according to Hernandez.

While Russia is a worry from a disinformation standpoint, so too is a sanctioned Iran, said Hernandez, who views Iran and North Korea as significant threats to our financial systems. "Practice makes them better," he said. William Rich expects Iran may attempt to skirt sanctions through cyber-enabled money laundering.[3]

Attacks and deterrents

According to Rich, governments look at cyber events to answer the following three main questions: 1) who perpetrated the attack (attribution), 2) will a response deter future attacks or make the situation worse (escalation), and 3) what intelligence could be lost by acting, said Rich. Successful attribution, which Rich has described as "a mix of art and computer science," makes the hackers' jobs harder.

By and large, deterrents are not working, said Kevin Kirst. "It works for the government and top banks, but other than that, no." Threat actors move on to regional banks where information sharing and intelligence may not exist. "The smaller banks get hit with the same malware that a big bank was hit with a few years ago," Kirst said. And if the smaller banks have access to reliable threat intelligence information, they don't always know how to action it, he said.

Sharing information is good offense…

There is plenty of information out there on cybersecurity; however, few people are willing to distill it, according to Don Ulsch. The evolving nature of the threat makes it hard to keep up. Ulsch urged firms to understand where you fit in this "neighborhood of cyberattacks." If you want to be compliant, if you are regulated by the Securities and Exchange Commission (SEC), and have cyber risk, you need to focus on what is it *you need* to understand about the risk and what you should be disclosing, he said. Ulsch recommends working with industry peers to better understand your collective obligations.

Ryan, a self-described auditor, identified three lines of defense. For the business itself: understand the risk, implement proper controls to address those risks, and then consistently operate those controls. The second line is to establish a dedicated risk management team within the broader risk function to independently identify risk and make sure mitigation controls are in place. Finally, the third line role of audit is to understand risk and make sure controls are operating effectively.

---

[3] *See* William Rich, "Iran Is a Threat to the Banking System," *Bloomberg*, October 25, 2018, https://www.bloomberg.com/opinion/articles/2018-10-25/iran-is-a-threat-to-the-banking-system.

..but it does not equal intelligence

Compliance is not the same as cybersecurity, and a threat doesn't wait for you to be compliant, Hernandez said. "If we try to equate compliance to cybersecurity, we will continue to chase threats."

Even with all the tools in place and an understanding of the law, there are inevitable pain points that can slow down a cyber investigation, said Kirst, who advises firms to think globally not locally. "US eyes can't look at Swiss data, for example. Japan does not agree that ransomware is a crisis," he said. "If you have an incident response retainer, use it."

Much of cyber risk is geopolitical in nature, said Ulsch. Organizations need to think about where they have assets globally and where there may be higher risks and varying roles of security. What may seem like a great opportunity to set up shop abroad with tax breaks, favorable labor rates, etc., could increase your vulnerability to cyberattacks, he said.

The financial picture

Large financial institutions are perfectly designed to be hard to defend, said Rich. They have sensitive and valuable regulated electronic data and a large workforce with access to data. Add to that the possibility of an antiquated IT system that could be several systems patched together as a result of a merger, which makes you vulnerable. Distributed ledger technology, with synchronized controls, multifactor logins, layered with context-aware security features and access control could be one way to build resiliency. It may also be an easier sell to the board than a new IT system, he added.

Resiliency is gaining even more attention within the finance industry and regulators, according to Ryan. The Sony Pictures attack in 2014, involving 100 terabytes of stolen data, was a wake-up call. Sheltered Harbor, where Ryan is Managing Director, grew out of the Hamilton Series,[4] a tabletop exercise meant to answer the question: could this happen in banking? The conclusion was "yes, it's a problem," Ryan said. Sheltered Harbor has established standards on backing up customer data, portability of data, inoperability, and recovery on an alternate processing platform. Resiliency is the ability to withstand an attack and to quickly recover from an attack, he said.

One way to build resiliency is to find a lawyer who is "comfortable with a crisis," before the crisis hits. You need someone who can communicate calm, Joves said.

Collective responsibility for safeguards and controls

Governance and oversight within an organization means cybersecurity is something we are all responsible for, said Ryan. Investors and shareholders may challenge boards to be accountable in the event of a material breach, and find themselves defending a class action lawsuit. In 2018, the SEC issued guidelines about public companies' disclosure obligations under existing law with respect to

---

[4] An exercise led by the Financial Services Sector Coordinating Council in coordination with the US Treasury Department and with support from the Financial Services Information Sharing and Analysis Center. *See* Tim Ryan, "Financial firms collaborate to defend against cyber-threats," *Compliance Week*, February 21, 2018, https://www.complianceweek.com/news/news-article/financial-firms-collaborate-to-defend-against-cyber-threats.

matters involving cybersecurity risk and incidents.[5] A robust cyber risk management strategy may help defend a class action litigation, Ulsch said.

Changing the culture of an organization is the hardest problem, said Hernandez. “The attack surface is only getting bigger, there’s a lot more data,” he said. It is incumbent upon organizations to understand the threat and impact, said Ulsch. “We need a better understanding of actions we take when do very simple things like click on an email. More crimes are committed by clicking on a link than what North Korea is doing to us,” he said.

In terms of industry preparedness, the panelists ranked the defense industrial base with its access to ‘insider baseball’ and telecoms as the strongest in terms of ability to defend, followed by our nuclear command control, the energy and power sectors, and transportation. The pharmaceutical industry is getting up to speed quickly. Industries that have lots of challenges include manufacturing and retail.

Our critical infrastructure and the interdependency of systems is our Achilles heel and hackers are good at finding the seams within our sectors, Hernandez said. He recommends building sophisticated public/private partnerships to bring resilience to other sectors that may not be as strong. Other countries are way ahead of the US in terms of the cyber workforce. It’s imperative, we figure out how to increase our own workforce and leverage our technology, he said.

Contact

Kevin Kirst
Principal
Washington, DC
+1-202-662-3865
kkirst@crai.com

[5] US Securities and Exchange Commission, “SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures,” news release, February 21, 2018, https://www.sec.gov/news/press-release/2018-22.