RSA

WHITE PAPER

STRATEGIES FOR MANAGING RANSOMWARE RISK IN FINANCIAL SERVICES

Disruption is rampant in the global financial services industry. Global economic challenges, profitability constraints, entry into new markets, the fluid regulatory environment, scrappy fintech startups and rapid changes in the way consumers manage their money are all changing how financial institutions adapt to the digital world. These factors are challenging the status quo in legacy brick-and-mortar banking relationships as banks transition to a digital ecosystem for money movement.

Financial institutions are investing in innovation, modernizing their business and infrastructure, and expanding their digital ecosystems via third-party tools and partners. These activities expose them to increasing cybersecurity risks that could impede their digital transformation initiatives and other efforts to meet the demands of digital customers. A growing security challenge for financial institutions is the recent uptick in ransomware attacks. In fact, in 2019, financial services represented 25% of all malware attacks.[1]

A growing security challenge for financial institutions is the recent uptick in ransomware attacks. In fact, in 2019, financial services represented 25% of all malware attacks.[1]

Ransomware attacks are growing more common in the financial services industry for a variety of reasons. For one, ransomware is simple to create using off-the-shelf toolkits, it's easy to deploy and is highly effective. The American Bankers Association states that ransomware "…offers cybercriminals an extremely low-risk, high-reward business model for monetizing malware."[2] Unlike other forms of malware, it doesn't have to be perfect or remain concealed on an organization's network for long periods of time. It's typically distributed through phishing, downloads, and compromised and fraudulent websites. Phishing has come a long way from the awkward, misspelled specimens that first emerged in the early 2000s. One notable example was a sophisticated phishing email that impersonated compliance officers and affected multiple credit unions in the United States in February 2019.[3]

WHY ARE THEY PICKING ON US?

Ransomware is hitting the financial services industry particularly hard in part because attackers know FSIs have both the means and the incentive to pay hefty ransoms. After all, financial institutions must keep money moving. Paying a ransom could mean they can do that and hopefully make the issue go away quietly, without attracting public or regulatory scrutiny. However, each institution must assess the risks associated with their actions to determine if they would choose to pay or not. There are many factors at play such scope and scale of the attack, the potential for the attacker to not follow through to decrypt—leaving them with continued disruption and cost in time and dollars to restore the information on their own. Obviously, any organization should work hand in hand with law enforcement with any of these types of incidents.

To further complicate matters for FSIs, several prominent ransomware actors have started publishing data they stole from organizations that chose not to pay the ransom in order to shame them.[4] The publication of these incidents on the dark web marks an important shift, as many organizations that had not previously reported these attacks may now be obligated to do so under various data privacy laws. This kind of "shaming" tactic—and the reputational and regulatory risks it creates—puts even more pressure on financial services organizations to have a strong ransomware mitigation strategy.

THE COST OF A RANSOMWARE ATTACK

Given the reputational and regulatory damage a ransomware attack can trigger, it's clear the total cost of ransomware extends far beyond the sum of the ransom. In assessing the risk a ransomware attack may create, FSIs must consider at a minimum the cost of lost productivity, lost revenue or profits, the impact of an attack on the institution's share price, the cost of reconstructing data, and legal or regulatory fines.

YOUR STRATEGY FOR MITIGATING THE IMPACT OF RANSOMWARE

RSA recommends a multi-pronged strategy for addressing ransomware that focuses on prevention through employee training and improved access controls, rapid detection and response, data backup, and building business resiliency.

PREVENTION

Preventing ransomware attacks is not easy, especially for large financial institutions. Since so many of these attacks originate as phishing emails, much of prevention hinges on educating your organization's entire workforce, which may number in the hundreds of thousands, to be more aware of these types of attacks and the tactics attackers use to perpetrate them. Indeed, a 2018 report from KnowBe4 found that 23% to 28% (or roughly one in four) of employees inside financial services companies are susceptible to phishing attacks. With awareness training, far fewer are susceptible: the number drops to 9% to 15% of financial services employees.[5]

A 2018 report from KnowBe4 found that 23% to 28% (or roughly one in four) of employees inside financial services companies are susceptible to phishing attacks.

But phishing isn't the only way ransomware is getting in. Attackers are also exploiting identities and weak passwords. Financial services companies have long implemented multi-factor authentication (MFA) to protect sensitive assets and data; they may need to consider expanding those implementations across the entire organization to protect all access, given the interconnected nature of today's IT infrastructures and how access to one system can quickly lead to others. While traditional authenticators, like hardware tokens, may have been cost-prohibitive and difficult to manage at the scale of a multinational FSI, modern mobile MFA on a smartphone is often simpler for users and administrators, and helps to minimize—if not eliminate—organizations' reliance on vulnerable password-based access controls.

KEY TAKEAWAY: Stronger security and access controls combined with training and awareness programs can minimize the human factor risk associated with ransomware.

RAPIDLY DETECT AND RESPOND TO RANSOMWARE

To lessen the impact from a ransomware attack, institutions must be able to rapidly detect the malware and prevent it from spreading across the network. This requires deep visibility across networks into endpoints, web applications and other infrastructure (both virtual and cloud-based).

Getting this level of visibility can be difficult for large financial organizations with complex IT infrastructures. Arming security operations staff with intelligent security platforms that leverage artificial intelligence to analyze and identify anomalous behavior and malicious code is critical. Ensuring that security operations staff can quickly prioritize and investigate real threats versus spending time analyzing false positives can accelerate mean time to detect and respond. Once a threat is detected, the ability to quickly and automatically orchestrate a security response is essential to minimizing the spread of ransomware and reducing its overall impact.

KEY TAKEAWAY: Organizations will never be able to completely stop the threat of a ransomware attack, so they must have appropriate threat detection and response capabilities to be able to reduce time to detection and automatically orchestrate a response to remediate the threat.

BACK IT UP

Backup is also a critical component of any ransomware mitigation program. Data should be backed up as close to real time as possible to minimize loss once recovered. Equally important: segmenting data backups from production systems. Institutions absolutely do not want a threat actor to be able to get to data backups, as that will nullify recovery attempts. Organizations should seek out cyber recovery solutions that include policy-driven automated workflows for moving and locking down business-critical data into isolated environments and enabling tools that incorporate artificial intelligence and machine learning analytics methods within a cyber recovery vault. And finally, cyber recovery solutions must be able to automate workflows to perform data recovery and remediation after a cyber incident.

Consider the impact of data loss on a global financial institution. If an institution was attacked and unable to recover data after a ransomware attack and became insolvent, this could lead to a run on the bank by customers and uncovered credit and liquidity positions with counterparty banks. The end result? A cascading worldwide financial crisis that could only be stopped by central banks stepping in, as they did during the 2008 financial crisis. In the “old days,” banks backed up their data on magnetic tapes and physically stored those tapes off-site. Today, financial institutions back up data via electronic networks, which can introduce incremental risk if attackers traverse both internal and external networks.

Organizations should seek out cyber recovery solutions that include policy-driven automated workflows for moving and locking down business-critical data into isolated environments and enabling tools that incorporate artificial intelligence and machine learning analytics methods within a cyber recovery vault.

BUILD RESILIENCY

Recovery from a ransomware incident is essential but insufficient on its own. Given that financial institutions must operate 24/7, ransomware attacks and the disruptions they cause are pressuring financial institutions to move beyond recovery and make resiliency their goal.

Building resiliency requires preventive and risk-driven planning, weaving resilient measures into the organization's business model, aligning security incident response and crisis management, coordinating business and IT recovery, and developing post-disruption strategies to reduce the impact of future disruptions.

Technology also helps to support a rapid response that leads to other important business outcomes, such as minimizing disruption to customers, maintaining liquidity and capital availability, and preventing widespread economic impacts. Organizations must consider their recovery time objective (RTO) as well as the amount of data they can afford to lose. This includes data that the organization and its third parties are generating and potentially losing.

Achieving resiliency also requires practice, and Quantum Dawn V is a shining example of this. Quantum Dawn V simulated a systemic ransomware attack on the financial sector. More than 600 participants from 180 financial institutions and government agencies across the globe participated in the simulation to test their collective response. This type of cyber war-gaming exercise is more important than ever, given how interconnected the global financial system is today. Quantum Dawn V, and indeed previous Quantum Dawn exercises, show how a large-scale cyber attack on the financial services sector could trigger a global economic crisis.[6]

While industrywide simulations like Quantum Dawn are critical, it's just as important for individual FSIs to identify their plans, processes, technology requirements, alternate financial counterparties, risk appetite and critical functions so that they can respond to singular incidents affecting their own institution.

KEY TAKEAWAY: Preparation and planning are critical elements to minimizing the impact of a ransomware incident. Financial institutions must have a well-documented and exercised business resiliency plan that spans business operations, technology capabilities and risk management to remain resilient in the event of an attack.

Given that financial institutions must operate 24/7, ransomware attacks and the disruptions they cause are pressuring financial institutions to move beyond recovery and make resiliency their goal.

CYBER INSURANCE

Cyber insurance may or may not help you minimize the cost of a ransomware attack. It depends on the policy. Some policies specifically exclude paying the ransom due to the moral hazard. Others will pay it. For organizations with such policies, CFO magazine explains that "working with the broker and insurers to understand the policy and the procedures for filing a claim is crucial to payment under the policy. Often the policies are tightly drafted to mitigate the impact of cyber fraud and require the policyholder to educate its workforce and implement appropriate means, such as business continuity and disaster recovery procedures, to prevent the ransomware intrusion and mitigate the impacts of an incident."[7]

BOTTOM LINE: If your institution chooses to leverage cyber insurance, you must understand the scope and requirements under the policy specific to ransomware in order to clearly acknowledge the level of risk your institution must accept, even with the buttress that the policy provides.

HOW RSA CAN HELP FINANCIAL INSTITUTIONS IMPLEMENT A RANSOMWARE MITIGATION STRATEGY

The global leader in digital risk management, RSA is helping the world's largest financial institutions, as well as regional and community banks, address ransomware and minimize cybersecurity risks through an integrated risk management program. The RSA portfolio is unique in its ability to bridge security and risk management functions.

With respect to preventing and minimizing the impact from a ransomware attack, RSA provides:

- **Modern, mobile** multi-factor authentication through RSA SecurID® Access. This makes it harder for attackers to exploit users' identities or compromised credentials to perpetrate a ransomware attack. RSA SecurID Access also paves the way for a passwordless environment that maintains strong security without inconveniencing users.
- Advanced threat detection and response through RSA NetWitness® Platform. RSA NetWitness Platform gives security teams at FSIs the unparalleled visibility they need to detect ransomware and other forms of malware on the network, endpoints, and across virtual and cloud environments. It also provides orchestration and automation capabilities to accelerate response and remediation.
- **An industry-leading integrated risk management platform**. RSA Archer® Suite helps organizations identify, assess and manage a range of risks to their business. It includes a use case for business resiliency that makes it easier for organizations to identify their most critical business processes and technologies, document business resiliency plans, and coordinate a cross-functional response

Financial services firms must look at a multipronged approach to minimize the opportunity for attack, to be able to rapidly identify when malware is present in the complex and expanding IT environment and be able to remain resilient when the attack occurs.

As a Dell Technologies company, our security and risk management solutions are complemented by Dell Technologies Cyber Recovery Solutions and Services to deliver resilient operations and backup systems that provide quick recovery from ransomware attacks.

Ransomware is a major issue in today's financial sector—especially as these institutions rapidly adopt new digital technologies to better serve their customers and compete in the digital era. Institutions must understand that there isn't a single silver bullet that can minimize the risk and impact of a ransomware or malware attack. Instead, financial services firms must look at a multipronged approach to minimize the opportunity for attack, to be able to rapidly identify when malware is present in the complex and expanding IT environment and be able to remain resilient when the attack occurs. Financial services will never be immune to cyber attacks and must face the fight on many fronts to protect their reputation of trust and continue to provide access to capital to their customers that rely on.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. Find out how to thrive in a dynamic, high-risk world at rsa.com

1 Calvin Hennick, "Cybercriminals Step Up Malware Attacks Against Financial Firms," BizTech, https://biztechmagazine.com/article/2019/09/cybercriminals-step-malware-attacks-against-financial-firms

2 Israel Barak, "Ransomware 101: What Banks Can Do To Mitigate Risk," American Bankers Association, (https://bankingjournal.aba.com/2018/07/ransomware-101-what-banks-can-do-to-mitigate-risk/ (July 20, 2018)

3 "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

4 Brian Krebs, "Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up," Krebs on Security, https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/#more-49994 (December 16, 2019)

5 "2018 Phishing By Industry Benchmarking Report," KnowBe4

6 "Global Banks Model Doomsday Ransomware Scenario," Finextra, https://www.finextra.com/newsarticle/34732/global-banks-model-doomsday-ransomware-scenario/security (November 8, 2019)

7 Michael R. Overly and Aaron Tantleff, "How to Mitigate the Threat of Ransomware," CFO.com, https://www.cfo.com/risk-management/2016/08/mitigate-threat-ransomware/ (August 31, 2016)