Prepare your financial institution to counter a new age of cyber threats

Protect institution and client assets through proactive testing and rapid response

Contents

Community banks and credit unions are increasingly facing a complex cyber threat landscape and the vast majority of these institutions aren't prepared to prevent or respond to cybersecurity attacks. As vulnerabilities increase, it's apparent that these banks lack the basic security capabilities in their technology and personnel that can help them fend off complex threats. Bad actors are aware of these financial services firms' susceptibilities and increasingly target them due to their lack of cyber capabilities and inability to respond to major cyberattacks.

Go on the offensive to counter modern threats

The security landscape for small and medium-sized financial companies is challenging. Attacks commonly come from state-sponsored bad actors; these groups are organized and supported by powerful world governments with the sole intent of attacking and stealing from financial firms. The resourcefulness of these groups can't be understated, but, while threats more commonly come from a distance, they can be active right next door, and your firm must be ready for both. Security threats are inevitable, routinely making national and industry headlines as seemingly ceaseless attempts are made to breach the defenses, at scale, of financial institutions. Smaller banks and credit unions are especially at risk in these efforts. Additionally, community banks and credit unions are facing an ever-growing amount of regulatory scrutiny and are struggling to deal with the requirements placed on them to demonstrate readiness for a major cybersecurity attack.

Small and medium-sized financial firms are largely unprepared for the sophisticated attacks being deployed against them. They don't have runbooks, response plans or crisis management plans. Employing each of these procedures is a base requirement of a proper security plan. In many cases community banks and credit unions don't even have a chief information security officer (CISO) in place, which places them in an extremely vulnerable situation.

Attackers often target thousands of users at once, drawing small amounts of money from each, but with total amounts that can equate to potentially thousands and millions in losses. Such methods make it very difficult to track or be prepared for pending attacks.

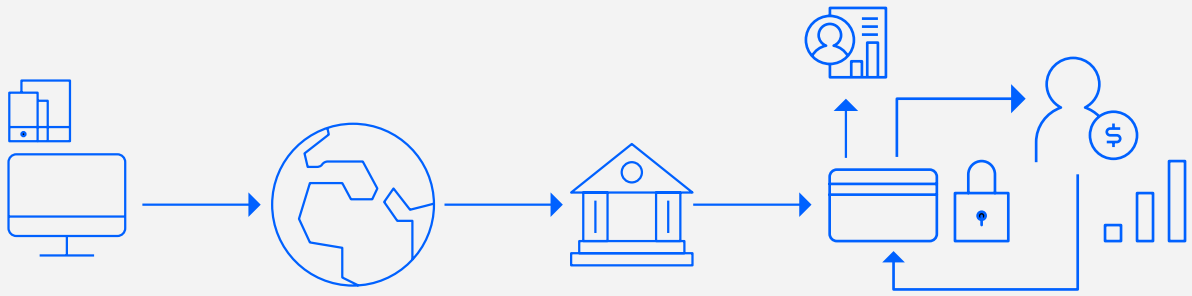
"Financial security firms are reportedly hit by security incidents a staggering 300 times more frequently than business in other industries." Identify Theft Resource Center.

So how do these attackers get in? There are near-countless methods that can be used, but it's most important to protect against those methods that are mostly commonly used.

Cyber attacks targeting individual institutions, and expanding to systmatic attacks impacting the entire industry

Limited budgets and insufficient tools to address evolving cybersecurity threats

Smaller cyersecurity teams compared to larger FSS institutions, and training and skills gaps



State sponsored targeting financial institutions, customers and third party providers who are crucial in providing security services

Increased state, federal and international regulatory and compliance requirements

Inadvertent insider threats frequently from social engineering and poor security fundamentals. These are often excecutives who are insufficiently focused on cyber hygiene

As deadlines mount, application development and updates can be rushed, leading to potential vulnerabilities that attackers can take advantage of. Additionally, many attackers will breach the personal accounts of your employees to take on the persona of a trusted advisor. They'll use this access to reach out to your customers, appearing as a bank representative, and gain knowledge and information that can lead to breaches and theft. Lastly, outdated systems that aren't prepared to meet the shifting attack methods of intelligent attackers are also potential entry points.

Good security hygiene is important but remaining secure through traditional security measures is a thing of the past. However, by going on the offensive, and properly preparing your organization for potential exposure, you can reduce the overall risk to your institution as you thwart attackers with preemptive measures.

Understand attack methods to better avoid threats

Small and medium-sized financial companies, such as community banks and credit unions, face a different set of security challenges than their large industry counterparts. Their security leaders are expected to protect the company as they would a larger organization, yet with less resources and budget. They're too dependent on the third-party services they currently employ, and those services lack the proper controls and testing. These third-party services make it difficult to communicate with them in the event of a breach and there are concerns whether they'll really work to protect organizations when a breach does occur. So, with all of these issues, how can small and medium-sized financial companies achieve the same level of protection as larger firms?

Threats from a single source can impact multiple targets

There's an increasing threat vector developing around a "systemic cyberattack." This type of cyberattack doesn't target just an individual financial institution. Rather, it targets an entire group of banks, as well as their infrastructures, software providers and other third parties that are paramount to run the US banking and payment industry.

Look inside your organization for inadvertent or deliberate threats

When it comes to cybersecurity, financial executives and employees can be their own worst enemies. For example, they or their family members may post information on social media that seems innocent but can be useful to an attacker. Or, some executives may skip security testing engagements or not adhere to security policies.

The number of inadvertent insider actions that benefit attackers is always increasing, and this number is primarily parallel with the rise of social media platforms and poor cybersecurity fundamentals. And these cases are not limited to newer, less-seasoned employees, but can emanate more often from the most senior executives in a financial services firm.

However, more serious threats can be purpose-driven as some of the larger attacks that have been made on financial institutions originated from the inside. Bad actors routinely target dissatisfied employees, offering them hundreds of thousands of dollars in exchange for disclosing sensitive data that can help them bypass security measures. So, one of the most concerning issues in security today isn't always keeping threats from the outside at bay, but knowing who to trust and how to counter threats exposures that originate from inside your organization.

Prepare yourself to prevent or resolve attacks

IBM X-Force® Red is an IBM Security team of veteran hackers that's hired to compromise financial organizations using the same tools, techniques, practices and mindset as attackers. They've seen firsthand how financial executives may elevate the risk of a compromise and understand what attackers may do with the information they find.

Through attacker reconnaissance, or open source intelligence gathering, attackers research targets from an external viewpoint to see what kind of information is publicly available, and then leverage that information to compromise the target. X-Force Red does much the same thing. But its target is the attacker.

The vast majority of banks are looking to the cloud for their modern security needs. And when coupled with the benefits of a managed service, your firm can enjoy the peace of mind that comes with a fully managed, comprehensive offering built and maintained by experts. Consistent support from an expert third party helps replace the unknown with the known and allows your firm and its representatives to further focus on the needs of your primary business and its customers.

IBM is soon launching these capabilities in an effort to support banks that have limited funding, resources and process to counter today's security threats. This service will include threat detection, response, artificial intelligence (AI), machine learning (ML) and much more.

IBM Security services package for small and medium-sized financial companies also includes X-Force Red vulnerability assessments, attacker reconnaissance and access to the IBM X-Force Command Center.

Assess the vulnerabilities of your institution from within

The vulnerability assessment service works to audit your institution to help identify areas where potential breaches or leaks may occur.

Attackers are not only stealing your employees' data through mishaps on social media platforms and elsewhere, but they're ingeniously stealing your customer's data, as well. And while much of the reasons for that theft is uncontrollable by your employees or institutions, you can implement measures to help prevent attackers from using stolen data in their attempts to access accounts and steal funds.

IBM takes steps daily to help ensure that potential breaches are swiftly identified and nullified. If an identified intrusion can be tied to a specific customer or employee's personal information or activities, that information is relayed to top personnel in the company.

Preventing further attacks starts with proper training of all personnel. But, when compared to larger financial services companies, smaller financial services firms have huge training and skills gaps that makes them especially vulnerable. X-Force Red puts the power in your hands with proper guidance on best steps all employees can take to avoid release of sensitive data. This training includes instructing employees on warning signs that they can report, when seen, to help prevent use of any data they may have mistakenly leaked or breach they may have allowed to occur.

Act as the attacker to stay ahead of potential attacks

Due to the small footprint of most small and medium-sized financial institutions, attackers do have less paths available that would lead to a breach of your defenses.

So, attackers perform aggressive open source intelligence gathering to collect information about people or companies that they can then use to compromise the target. Their targets, such as small and medium-sized financial companies, should be doing the same.

X-Force performs attacker reconnaissance, which is the process of sweeping the most common sources where sensitive data is leaked. This process means IBM works to identify the leaks that attackers could use before they can use that information to damage your institution.

Attackers look for publicly available data in the following places and in many other areas:

- Social media
- Dark web
- GitHub
- Shodan
- Censys
- Home pages
- Open port searches
- PDFs

Train your teams to better prevent or act against threats

Hundreds of commercial organizations have visited the IBM cyber range during its first year of operation. Built to teach critical cybersecurity-related crisis leadership skills in a realistic environment, the cyber range helps participants experience and work through the stages and effects of a breach.

Using its expertise, IBM Security recreates events within your construct of tools, organizational structure, processes and playbooks.

IBM X-Force Incident Response and Intelligence Services (IRIS) can create a customized cyber range experience that tests your existing response procedures. What's more, the cyber range can come to you, allowing you and your teams access through a semi-customized onsite experience with modules. You can participate in the cyber range at locations, such as client hotels, client sites, by remote, or at the primary IBM X-Force Command Cyber Tactical Operations Center (C-TOC).

Take the next steps to better protect your customers and assets

Community banks and credit unions must focus on the following key security modernization strategies when addressing the cybersecurity threat landscape:

- Invest in security intelligence and defenses that use automation, AI and advanced analytics.
- Increase the focus and capabilities of your fundamental security practices.
- Collaborate with industry peers and experts to create and foster a security-rich culture.
- Involve senior executives and boards in the planning and execution of security measures.
- Develop threat detection capabilities to protect against fraud and establish digital trust with clients and business partners.
- Participate in cyber range exercises where you'll test your cyber incident response (IR) plans.
- Define your security capabilities in the "shared responsibility" model as your company adopts hybrid cloud.
- Perform a vulnerability assessment to gain knowledge of any security gaps.

Given the limitations that community banks and credit unions have in terms of skills, funding and security capabilities, it's imperative that you choose a security partner who can provide end-to-end integrated security capabilities. These capabilities should accelerate deployment, simplify threat detection and ensure that there's a fully tested IR and crisis management plan in place.

Start developing modern security measures today

Due to the developing, yet still limited security capabilities of today's community banks and credit unions, cyber criminals and bad actors are focusing their efforts on this industry. As such, IBM recommends that all such member companies of this marketplace take the following steps:

1. Conduct a vulnerability assessment to better understand current security threats and risks.
2. Invest in threat detection capabilities and implement security information and event management (SIEM) technology.
3. Define IR plan runbooks.
4. Invest in an IR platform.
5. Perform tabletop and crisis management exercises to determine preparedness for a cyberattack.

Why IBM?

IBM has been a long-time strategic partner and provider to the financial services industry, which represents the largest industry vertical for IBM Security. Due to an increase in the volume and complexity of cyberattacks directed at smaller banks, IBM considers community banks and credit unions a strategic area of focus and is providing security products and services that target the unique regulatory and compliance requirements of this industry.

IBM focuses on vulnerability management, threat detection and IR as the three key pillars of its security offerings. These capabilities are available as a bundled offering, and with subscription pricing. IBM views the community bank

For more information

To learn more about IBM Security for community banks, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/waiting_for_updated_url. com.

Gary Meshell leads the worldwide IBM Security business in financial services and is responsible for sales, business development, offering management and the overall go-to-market strategy for IBM Security offerings in financial services.

Gary is a security and cloud thought leader within the financial services industry and has spoken on these topics in China, Russia, Brazil and other parts of the world. He's worked with many large insurance companies, international banks and investment management companies to support the design and implementation of their hybrid cloud and security programs.

Additionally, Gary leads the IBM financial services regulatory consortium, which consists of 33 financial services companies. These companies collaborate to form regulatory standards that can accelerate the deployment of the public cloud into the financial services industry. Gary has also worked closely with law enforcement agencies, such as the FBI and the United States Department of Homeland Security, to identify threats and potential attacks to the financial services industry. He also facilitated cybersecurity incident management exercises at the IBM cyber range facility for over 100 financial services companies.

IBM Corporation
IBM Financial Security Services
Route 100
Somers, NY 10589

Produced in the United States of America
October, 2019