Managing your cyber security risk

How prepared is your financial institution for a cyber attack?

Your customers want 24-hour access to their financial information, via smartphone, tablet, PC and ATM. Your employees and third-party service providers are given remote access to the corporate networks, which increases productivity and ultimately, the company's bottom line.

As financial institutions expand their network capabilities to allow more access to customers and partners and to meet global business requirements, the potential gaps, and therefore opportunities, for a cyber attack increase as well. No financial institution is immune to a cyber attack. But there are steps you can take to improve resilience, minimize risk, and most importantly, ensure you can detect, respond and remediate quickly to minimize damage.

Your customers, executives and shareholders expect it. Your organizational reputation and financial stability depend on it. And the organizations that regulate the financial industry require it.

In this white paper we'll provide you with the steps required to identify your cyber security risk, prepare a comprehensive incident response plan, manage vulnerabilities specific to third-party providers, and direct you where to find more detailed information on relevant guidelines.

Cyber security is a business issue and increasingly, an executive management issue

It's no longer just the IT professionals in a company that have to worry about information security incidents and data breaches. There's a lot of discussion among executive management and boards of directors about the fear of a cyber attack "keeping them up at night," but what is actually being done to address the risk?

The topic of cyber security needs to be a top priority on every board meeting agenda and in your company's overall business plan.

This not only makes good business sense, but Federal Financial Institutions Examination Council (FFIEC) auditors now look for evidence of board of director involvement during their audit process. Executive management sets the tone for how serious the company takes the issue of cyber security. You must ensure that everyone with network access is aware of your institution's security protocols and is trained on how to keep your company's data secure.

It's not a matter of "if" but "when"

A security incident will happen at your financial institution. The financial services and retail industries are consistently the top two targets of cyber criminals. The financial services industry is considered one of the most "high value" targets of cyber criminals because infiltrating the proprietary data of financial institutions ensures hackers one of the best monetary returns on their time investment. The cyber attacks that have occurred at well-known retail companies received significant media coverage, but represent only a small fraction of the many incidents that have taken place during the past few years. Criminally-funded gangs with intent to steal financial information continuously target financial institutions both large and small.

The two categories that make up approximately 70% of security incidents at financial institutions are:

1. Crimeware – The backdoor staging of advanced attacks and data stealing
2. Web App Attacks – Compromising customer accounts and hacking websites and databases

Today's hackers are sophisticated cyber criminals that are part of global organized crime organizations intent on stealing, spying, or just causing disruption to your business. And while these criminals may be sophisticated, they use fairly simple techniques to successfully access corporate networks.

Two-thirds of security incidents reported over the past two years have featured phishing, with a ninety percent **(90%)** success rate on phishing campaigns of **10 or more emails.**

Seventy-eight percent **(78%) of breaches** in 2014 were considered low difficulty with regard to the tactics used to **gain access**

Now that you know some of the statistics, let's turn our focus to a risk management solution beginning with a risk assessment. Answering the questions in step one will give a thorough understanding of what needs to be done to minimize your financial institution's risk.

Step one: it's time for a risk assessment

The risk assessment process should begin with executive management asking the managers of the information technology department the following questions:

- What kind of access is available to our financial institution and by whom?
- What security protocols are currently in place to control and monitor day-to-day access to these connections?
- Are there any legacy technology, security expertise, or budget issues that need to be addressed?
- Are we providing ongoing security awareness training to everyone that has access to our networks?
- Are we performing due diligence on all third-party service providers with access to our networks to ensure we are not exposed to security risks on their end?
- Are we in compliance with the FFIEC and National Credit Union Administration (NCUA) guidelines?
- Do we have a comprehensive incident response plan in place to use in the event of a security incident or data breach? How often is the incident response plan updated and how familiar are the key players with the process?

This last question is of particular importance because it is the most critical piece of your financial institution's security framework. It is the emergency guide you will rely on to get through a security incident or data breach in the most time-efficient manner and with the least long-term repercussions for your company. However, it is one of the security steps most neglected by financial institutions.

The FFIEC recognized this problem and issued new guidelines that recommend financial institutions develop a plan and continually test and update it in order to appropriately respond to attacks when they happen. The FFIEC also realizes that this skillset might not be available within the existing staff of financial institutions, so they recommend finding a capable incident response firm to partner with that can be onsite if and when an incident occurs.

"Financial institutions and their service providers should **anticipate potential cyber incidents** and develop a framework to respond to these incidents. If a financial institution or its Technology Service Provider (TSP) is under attack, **management should consider** the potential impact of any decision to limit or suspend processing and any downstream implications to the financial institution's business partners, customers, or other TSPs. Incident response processes **should also address concerns** regarding availability, confidentiality, and integrity of data with different sensitivities. Finally, the financial institution and its **TSPs should periodically** update and test their incident response plan to ensure that it functions as intended, given the rapidly changing threat landscape."

Source: FFIEC Business Continuity Planning: Appendix J: Strengthening the Resilience of Outsourced Technology Services, Incident Response section

Step two: create or update an incident response plan

A comprehensive incident response plan must include the following steps:

1. Verify that an incident or breach occurred
2. Maintain or restore business continuity
3. Reduce the incident impact
4. Determine the root cause of the incident
5. Prevent future attacks or incidents
6. Improve security and incident response
7. Prosecute illegal activity
8. Keep key stakeholders informed of the situation*
    a. Establish clear roles and responsibilities
    b. Determine lines of communication for an event
    c. Identify the response team and their specific roles

*The key players for a security incident (data compromise) will include IT and security personnel, including the CIO, CISO, and executive management. The list of key players for a data breach (confirmed disclosure) includes those involved with a security incident, as well as the following groups: the board of directors, the legal department, public relations, customer service, human resources, and law enforcement.

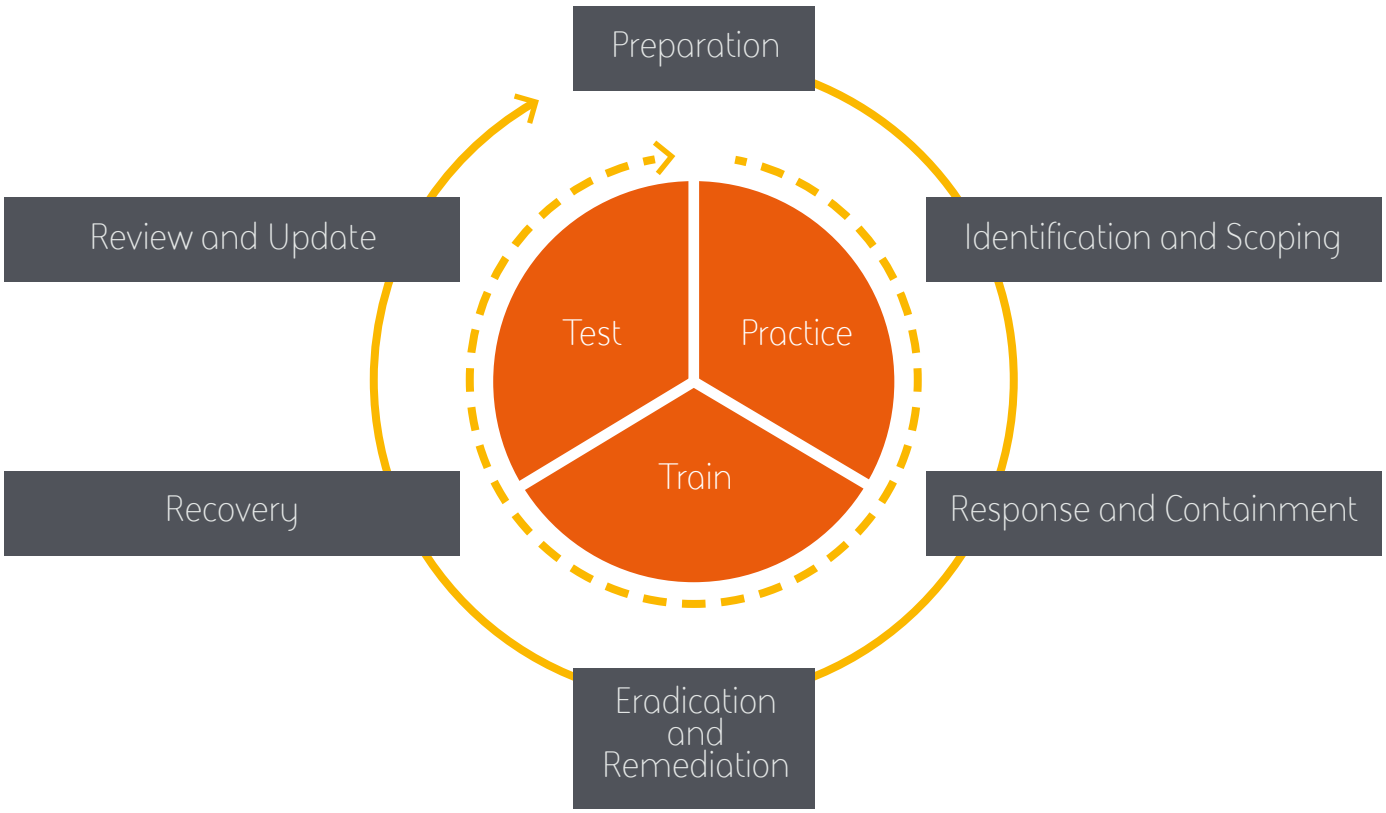
Step three: test the plan, review the plan, repeat

Now that you have an incident response plan in place, there will need to be periodic testing of the plan to ensure it is current and ready to launch. On a regular basis, check to ensure:

- The steps in the plan are still relevant
- Team members are properly trained and understand their responsibilities
- All key stakeholders work well together under pressure
- There is a reduced risk of a counteractive response during an incident
- Any outsourced responders are involved in the testing

Great. You have performed a risk assessment, created an incident response plan, tested the plan, and scheduled periodic testing of the plan with the key players.

Now that all of the practice is over and your financial institution is the victim of an actual cyber attack, it's time to put the plan into action. Once that's done, it's time to do a post-incident review to determine what worked and what needs improvement. All of this information should be documented and incorporated into the next plan revision.



The Six Steps of Incident Response

Step four: perform third-party due diligence

Most companies rely on third-party service providers in some or several departments of their organization. This is particularly true in the area of network security because of a shortage of highly qualified job candidates and the very competitive market to try to recruit and keep top talent. This is why it is essential that any third-party provider involved in the implementation or monitoring of your network security framework is properly vetted and follows all protocols and procedures required by the FFIEC.

> This is why **it is essential** that any third-party provider involved ... is properly vetted and follows all protocols

Step five: know what's required of you by federal regulators

Federal agencies are taking a very active role to combat cyber crime. It was announced in August 2015 that the National Cybersecurity and Communications Integration Center (NCCIC) is now part of the Department of Homeland Security (DHS). Other federal agencies like the FFIEC, NIST, and the NCUA are all devoting time and resources to the topic of cyber security. The result of their ongoing efforts is the online publication of very detailed guidelines by each agency. For example, the FFIEC recently released a cyber security assessment tool to help financial institutions identify their risk and determine their cyber security preparedness. The assessment tool was developed in response to the findings of a FFIEC pilot program in 2014 that evaluated the preparedness of 500 financial institutions to mitigate cyber risks.

We strongly recommend that you review the websites of these federal agencies for their detailed information about cyber security:

- FFIEC.gov: Cybersecurity Assessment Tool
- FFIEC.gov: IT Examination Handbook for Management
- NIST.gov: Computer Security Incident Handling Guide
- NCUA.gov: Letter to Credit Unions

Summary

A cyber attack at your financial institution is not a matter of 'if', but 'when'. It's time for the executive management and the board of directors to take a more active role in understanding and managing the cyber security risks. Start by including cyber security preparedness updates as a permanent topic at board of director meetings and implementing the recommendations in this white paper.

Most important, risk management has to be an ongoing discussion and an evolving process. Cyber criminals will continue to invent technology to penetrate networks, so financial institutions need to be vigilant about their ongoing readiness to combat these issues.

> Most importantly, **risk management** has to be an ongoing discussion and an evolving process

We are BAE Systems

We help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations.

We do this using our unique set of solutions, systems, experience and processes - often collecting and analyzing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We employ over 4,000 people across 18 countries in the Americas, APAC, UK and EMEA.

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
154 University Avenue, 2nd Floor
Toronto, ON
M5H 3Y9
Canada
T: +1 (647) 777 2000

BAE Systems, 265 Franklin Street, Boston, MA 02110, USA

E: learn@baesystems.com | W: baesystems.com/businessdefense

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST

CESG Certified Service Cyber Incident Response

CPNI Centre for the Protection of National Infrastructure