S|C SECURANCE CONSULTING

the advantage of insight

From Inception to Maturation:

Developing Agile, Sustainable Information Security Programs for Financial Institutions

www.securanceconsulting.com

Cyber attacks are no longer a matter of if, but when. Fledgling cybersecurity efforts focus primarily on managing risk, but it's equally important to identify attacks as they happen and recover quickly. Establishing a mature, dynamic information security program is essential to the health of all businesses and critical for the financial sector, where thieves can steal millions before anyone notices.

INTRODUCTION

Financial institutions are some of the most frequently attacked organizations. Cyber criminals have already stolen billions from banks and show no signs of stopping.

Banks face a triple burden when it comes to cybersecurity: complex infrastructure, high-value assets, and high expectations from customers and regulatory agencies. The size of the institution is irrelevant. Regional banks face as much risk as global institutions. In some ways, the risk is greater, because the cost per record stolen is higher, and there are fewer resources available to dedicate to cybersecurity.

The good news is that there is no correlation between the amount of money spent on security efforts and the safety of data or assets. The key is to implement a risk-based cybersecurity framework, designed to limit the damage of an attack and swiftly restore normal operations.

> "In the place of guns and masks, this cybercrime organization used laptops and the Internet."
>
> —Loretta Lynch, describing how cyber thieves stole $45 million from New York City

Years of research and innovation have led to the development of standards and best practices that protect data and enhance operations— streamlining procedures, reducing complexity, improving asset management, and eliminating manual processes.

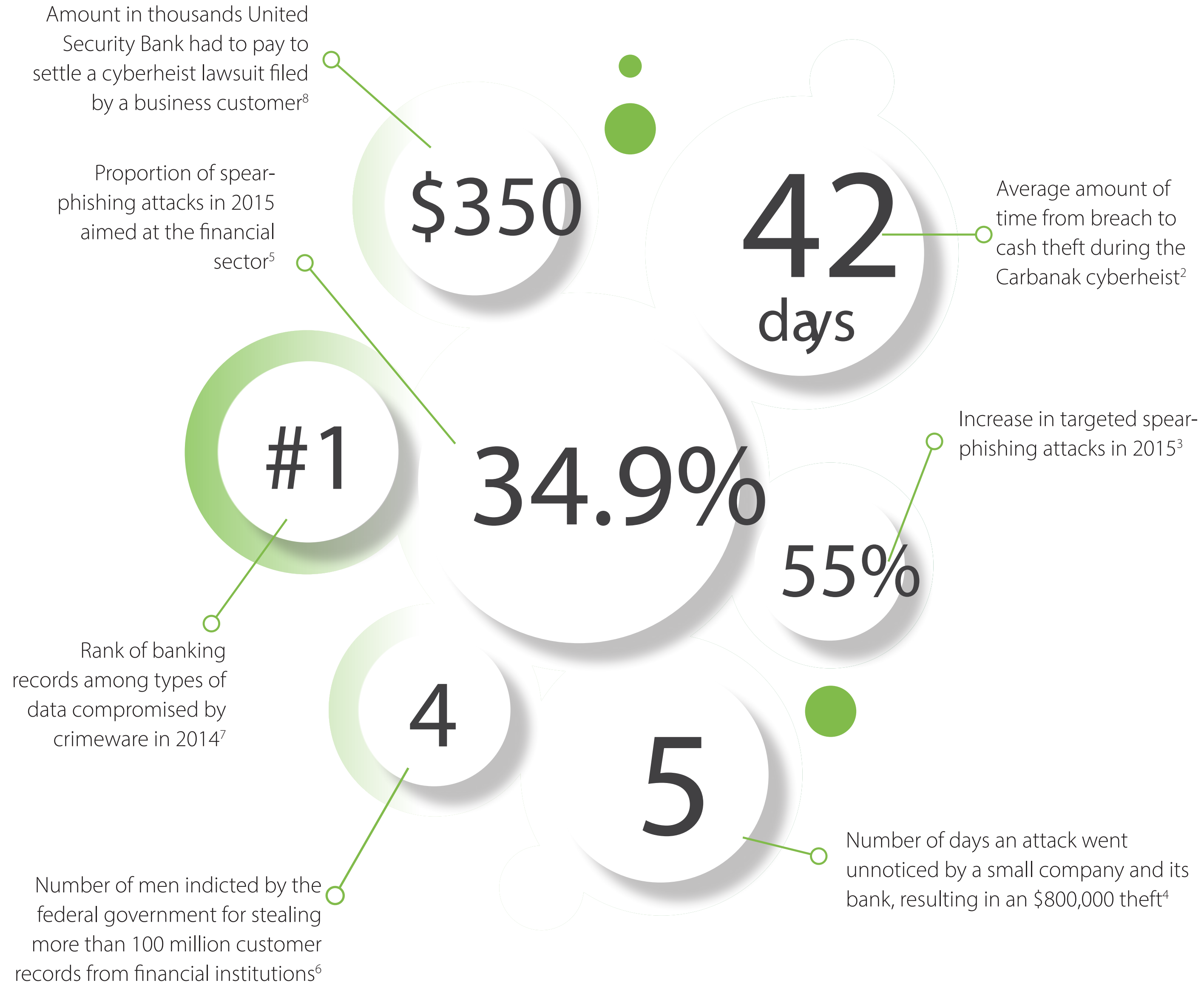
This paper details the components of a mature information security program and how implementation delivers benefits beyond security. To provide a general structure and standard set of terms, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is used as a reference point.

BANK ROBBERY 2.0

Bank robbers don't need to walk into a bank and hand the teller a note. They can reach into the vault from the other side of the world, and it may take months to notice they were there.

Starting in 2013, an international cartel of cyber criminals stole more than one billion dollars[1] from more than 100 financial institutions. The Carbanak campaign infected computers inside victim firms, using targeted spear-phishing and malware. Once inside, they carefully monitored how the banks operated and who was in charge.

Armed with this information, they impersonated bank officers, forced cash machines to dole out money to their confederates, and stole millions around the world. The attack relied on known exploits. If victim organizations had been properly patched or had active monitoring, they could have limited losses or avoided them altogether.



$350 — Amount in thousands United Security Bank had to pay to settle a cyberheist lawsuit filed by a business customer[8]

42 days — Average amount of time from breach to cash theft during the Carbanak cyberheist[2]

34.9% — Proportion of spear-phishing attacks in 2015 aimed at the financial sector[5]

55% — Increase in targeted spear-phishing attacks in 2015[3]

#1 — Rank of banking records among types of data compromised by crimeware in 2014[7]

4 — Number of men indicted by the federal government for stealing more than 100 million customer records from financial institutions[6]

5 — Number of days an attack went unnoticed by a small company and its bank, resulting in an $800,000 theft[4]

TAKE CONTROL OF CYBERSECURITY

Attacks are on the rise, and malefactors continue to make headway, but financial institutions can improve resilience and decrease recovery times by implementing a comprehensive information security program.

Meet hacker sophistication with security maturation

Cyber criminals, hacktivists, and foreign governments want access to the U.S. financial system, and every year they find new ways to improve their operations by automating systems, developing new exploits, and expanding their reach. Combat hacker sophistication by developing a plan to continuously improve cybersecurity and striving for the most mature information security program possible.

Meet expanding regulations with better administration

Government agencies frequently revise regulatory mandates and guidelines to keep pace with changes in technology and industry. Far from being a burden, regulations mandating a tightly controlled environment can be an incentive to make strategic investments that strengthen an organization. Implement strong controls that meet or exceed industry best practices to get ahead of hackers and regulators.

Meet high expectations with process modernization

Customers expect their accounts to be secure, but they also crave technology solutions that give them more access to those accounts. Phase out legacy systems that predate current security requirements and eliminate overly complex manual processes to satisfy customers and thwart attackers.

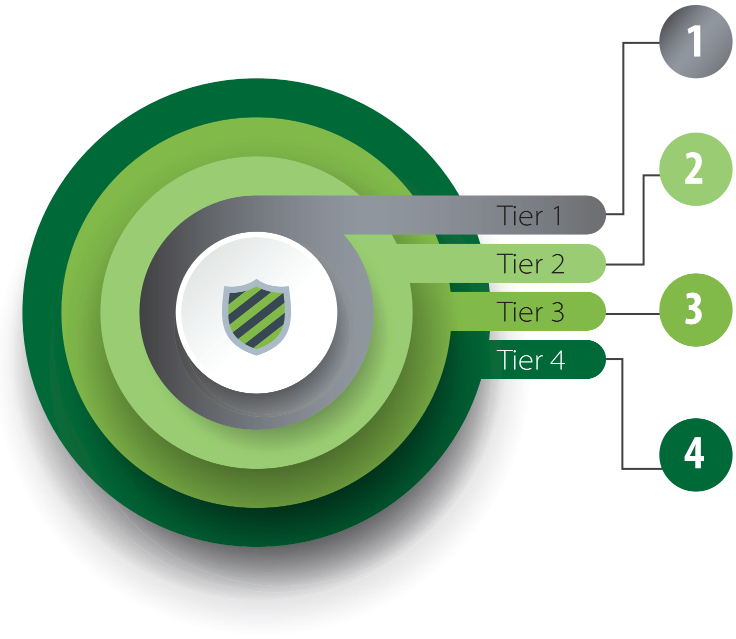
> “I am often asked about my list of ‘things that keep me awake at night,’ and I think it’s fair to say that cybersecurity is at the top of that list.”
>
> — Sarah Dahlgren
> Executive VP, Federal Reserve Bank of New York[9]

A FRAMEWORK FOR CYBERSECURITY SUCCESS

In 2014, NIST released a voluntary, risk-based cybersecurity framework for critical infrastructure sectors. They worked with hundreds of cybersecurity experts and businesses to develop a framework that establishes standard terminology for discussing cybersecurity, provides a flexible platform for businesses and governments to enhance information security, and encourages organizations of all sizes to participate.

The CSF's core Functions and security Tiers provide a common language for discussing the most important facets of an information security program and how mature it is within an organization.

CSF Maturity



1. **Partial**: cybersecurity and risk management processes are ad hoc and reactive; least mature.

2. **Risk-informed**: risk management processes are approved but not part of organizational policy.

3. **Repeatable**: risk management processes are expressed as formal policies, and cybersecurity efforts are updated regularly.

4. **Adaptive**: dynamic, organization-wide cybersecurity and risk management efforts focus on continuous improvement; most mature.

CSF Core Functions[10]

Identify
Understand how to manage cyber risk to data, systems, assets, and capabilities.

Protect
Implement controls and safeguards that ensure business continuity.

Detect
Implement active monitoring to identify attacks when they occur.

Respond
Determine what actions to take after a cybersecurity event takes place.

Recover
Create plans to restore services and capabilities and maintain resilience.

IT’S A BUSINESS ISSUE, NOT AN IT ISSUE

Banks manage financial and credit risks as a matter of course. Cyber risks should be treated the same way, with the same top-down level of executive and organizational support. It all starts with proper planning and good management, activities at which financial institutions excel.

Take the lead

Whether you hire a Chief Information Security Officer (CISO), engage outside services (virtual CISO), or work with in-house resources, executive-level authority is crucial to developing a mature cybersecurity program. The program will never be fully integrated with the business without that level of support.

Know your environment

The CSF’s core Functions begin with “Identify.” This is not a one-time event. Mature information security programs include thorough, periodic risk assessments to identify changes in technology and transformations in the threat landscape. Additionally, asset management should be continuous and integrated into daily operations. No technology should come into the environment or leave it without following documented procedures and assessing the risks associated with the change. It’s easy to forget that discarded systems, from servers to copiers, can be a valuable source of information to hackers.

$6 TRILLION

Amount that will be spent on Internet of Things (IoT) solutions by 2021. Companies are expected to adopt IoT devices more quickly than consumers.[11]

Keep your guard up

Protection begins with strong controls and well-defined policies and procedures. Governance is another area where leadership is crucial. Executive-level oversight ensures protective measures take business objectives into account, making the environment more efficient and more secure. Protecting data also means limiting access. If someone doesn’t have a valid business need to access specific data or systems, he should not have access. Loose access controls increase the likelihood of costly mistakes. Lastly, one of the best forms of protection is prevention. Proactive patch management and system maintenance significantly reduce the chance of attack. In 2014, 97 percent[12] of exploits took advantage of common vulnerabilities and exposures (CVEs) for which patches were already available.

Sound the alarm

Cyber criminals like to take their time. The worst damage usually comes days— or even weeks— after they breach your defenses. Continuous monitoring and detection processes are a vital component of any cybersecurity program. Regular penetration testing can help banks identify weak points and develop a greater understanding of how attackers gain access. Given that banks are subjected to a disproportionately large number of spear-phishing attacks, it’s a good idea to conduct phishing simulations to quantify the risk and develop targeted user education.

$18 MILLION

Amount ransomware cost Americans from June 2014 to June 2015. These attacks continue to grow and were the number-two form of malware in 2015.[13]

Prepare for the worst

The interconnectedness of the financial system, which is an advantage for customers and banks, precludes the possibility of impenetrable defenses. Be prepared to respond when (not if) an attack occurs. Create a response plan that outlines mitigation efforts and includes an analysis of the attack to understand the damage and the activities required to contain the breach.

Get back to business

Despite widespread understanding of the depth and breadth of cybercrime, businesses still incur significant reputational damage after an attack. One way to curb negative financial and reputational ramifications is to recover quickly and skillfully. Resuming normal operations is essential, but so is communicating with affected customers and regulatory and law enforcement agencies. Prepare draft communications ahead of time to avoid ad hoc blunders. Determine which systems have the highest priority in the event of widespread disruptions and who will be responsible for recovery tasks.

Organized criminals, hackers, and foreign governments want access to financial institutions, but establishing a mature cybersecurity framework makes it easier to prevent attacks or limit damage and recover swiftly when they occur.

$750 MILLION

Amount lost in the U.S. to spear-phishing attacks from October 2013 to August 2015. Banking information is among the most sought-after in these attacks.

BEYOND SECURITY

No bank wants to endure a damaged reputation or high recovery costs after an attack, but stakeholders need more incentive than avoiding adverse outcomes to justify significant cybersecurity investments. Luckily, enhancing security provides a host of related benefits that improve organizational performance.

Strong controls increase efficiency

Companies that institute agile, risk-aligned controls are more efficient, have greater operational stability, and perform better. This is even more true for small and mid-sized businesses that have fewer resources to squander on inefficient practices.

$272 MILLION

Number of stolen email username/password combinations recently sold by a single hacker. Thousands belong to employees of U.S. banking, manufacturing, and retail companies.

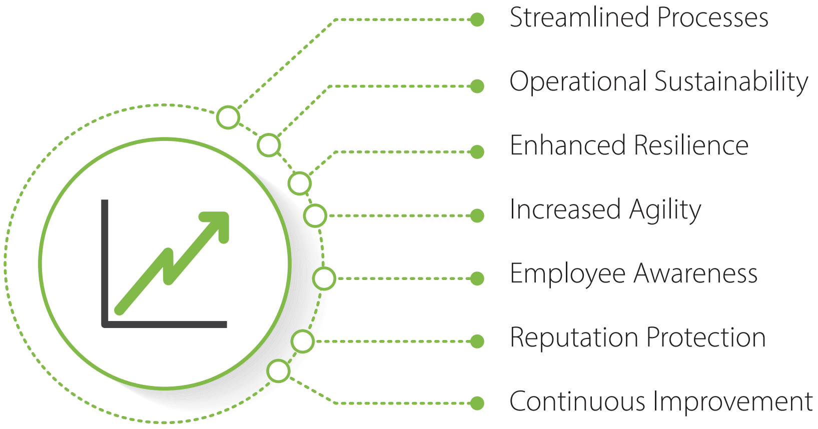
Information is power

Training employees to identify and avoid unnecessary risks and errors makes an organization more secure, but it also creates an empowered workforce that is more alert for errors and inconsistencies. According to Verizon's Data Breach Report, 29.4 percent of incidents[14] were the results of miscellaneous employee errors.

Security requires agility

Assessing the environment to identify risks and define controls is an opportunity to review operations and eliminate complex or outdated procedures. By implementing a continuous management and improvement cycle for cybersecurity, firms create a stable structure for the ongoing review of policies and procedures. Agility becomes an integral part of the culture.

Benefits of a Mature Cybersecurity Program



- Streamlined Processes
- Operational Sustainability
- Enhanced Resilience
- Increased Agility
- Employee Awareness
- Reputation Protection
- Continuous Improvement

BETTER SECURITY IS POSSIBLE

Cyber criminals want to maximize gains and minimize effort. While the number of attacks and the level of sophistication increases year after year, criminals continue to take the path of least resistance, making use of known exploits and vulnerable organizations.

Businesses that adopt an agile information security program designed to adapt to changing needs, place an emphasis on continuous improvement, and establish a cybersecurity culture at every level of the organization are harder to breach. They are also prepared to stop the attack and limit the damage when a breach occurs. Their defenses lower the profit margins for cyber criminals, making them less attractive targets.

Due to the efforts of researchers, industry experts, and the government, businesses have access to a wide variety of best practices and frameworks to guide the development of a mature security program tailored to their needs. The benefits of such a program extend beyond information security, enhancing efficiency and reducing complexity for the business as a whole.

> “While the threats against us may seem innumerable, infinitely varied, and ever changing, the reality is they aren’t. This certainly doesn’t diminish the significant challenges faced by defenders, but it does imply a threat space that is finite, understandable, and at least somewhat measurable.”

—2015 Verizon Data Breach Investigations Report

If your business is ready to improve security and resilience, our consultants can help. Contact us or visit our website to learn more about our services and to access resources, including white papers, articles, and our network security self-assessment.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

[1] New York Times, Feb 14, 2015

[2] Krebs on Security, Feb 15, 2015

[4] Krebs on Security, May 2013

[3,5,6] Symantec Internet Security Threat Report, 2016

[7] Verizon Data Breach Investigations Report, 2015

[8] Krebs on Security, June 2014

[9] https://www.newyorkfed.org/newsevents/speeches/2015/dah150324

[10] https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[11] https://www.businessinsider.com/internet-of-things-report

[12] https://enterprise.verizon.com/?cpur=1&

[13] https://www.computerworld.com/article/3065360/researchers-nab-millions-of-stolen-credentials-for-gmail-hotmail-yahoo-banking.html

[14] https://enterprise.verizon.com/?cpur=1&

From Inception to Maturation
Developing Agile, Sustainable InfoSec Programs for Financial Institutions

S|C SECURANCE CONSULTING
the advantage of insight

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com