SECURANCE CONSULTING
Advantage of Insight AI

Agility and Stability: Developing Information Security Programs for Financial Institutions

www.securanceconsulting.com

INTRODUCTION

Financial institutions are the second most frequently attacked organizations after healthcare and suffer particularly from credential and ransomware attacks. In the past year, 74 percent of Financial Institutions have experienced a rise in cyber crime.[1]

Banks face a triple burden when it comes to cybersecurity: complex infrastructure, high-value assets, and high expectations from customers and regulatory agencies. More and more, we are coming to understand that 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.

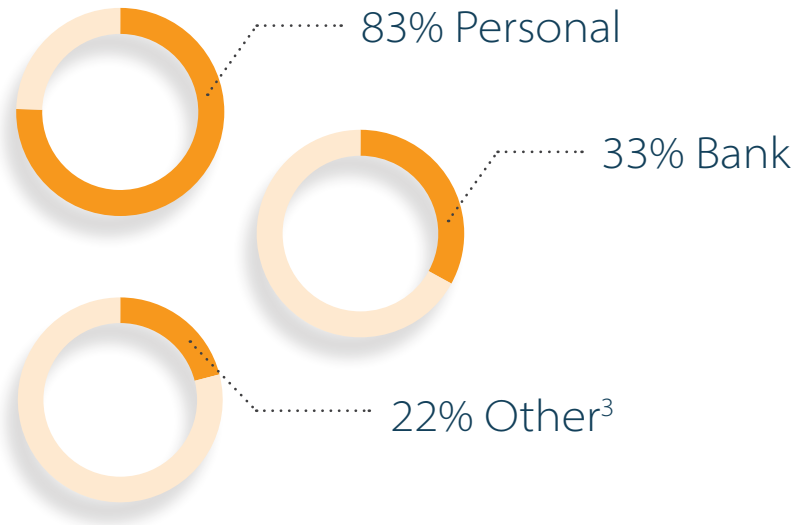
> The average total cost of a data breach in the financial industry in 2021 is **$5.72 million**.[2]

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.

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.

Data compromised in financial sector breaches:



BANK ROBBERY 2.0

Bank robbers don't need to walk into a bank anymore. They can reach into the vault from the other side of the world— and it may take months to notice they were there. Every year, attacks become more sophisticated and difficult to detect. The following are this year's top five threats in the financial sector:

1. Emotet – A Trojan that mainly spreads through spam emails containing malicious macro-enabled documents or links. Allows criminals to monetize attacks via information stealing, email harvesting, and ransomware distribution.

2. Dridex – A Trojan that acts as a banking credential stealer, ransomware delivering system, and remote access control tool. Often delivered through macro-enabled Office documents attached to emails.

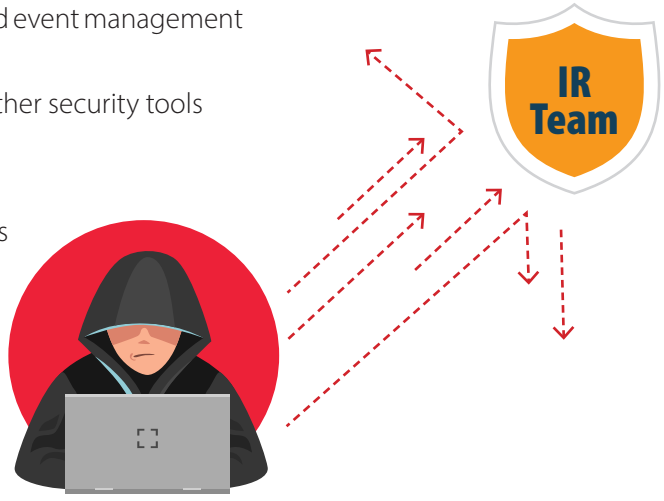
3. Trickbot – A threat that targets the financial sector, providing modules that support the theft of banking credentials and cryptocurrency, as well as ransomware.

4. Qbot/Qakbot – A versatile threat that supports several modules (from remote access to credential theft). Qbot can observe email threads and inject itself into existing threads, increasing the chances that a user would deem malicious attachments as legitimate ones.

5. Hancitor – Primarily acts as a delivery mechanism for other threats and often uses DocuSign documents to entice targets into activating malicious attachments.[4]

In many cases, cyber robberies become hostage situations. To defeat incident response (IR) teams, cyber criminals have begun engaging in what are known as counter-incident response strategies. When the IR team begins to defend against a breach, the cyber criminal now knows there is an active adversary disrupting the attack and takes action to subvert IR efforts. This action might take the form of any of the following:

- Blocking events from hitting the security information and event management (SIEM) system
- Disabling the Antimalware Scan Interface (AMSI) and other security tools
- Clearing logs
- Manipulating time stamps
- Using alternative authentication material, such as pass the hash/ticket
- Using a signed binary proxy execution (e.g., LOLBins)
- Using legit files to execute untrusted code
- Deploying ransomware
- Deploying wipers[4]



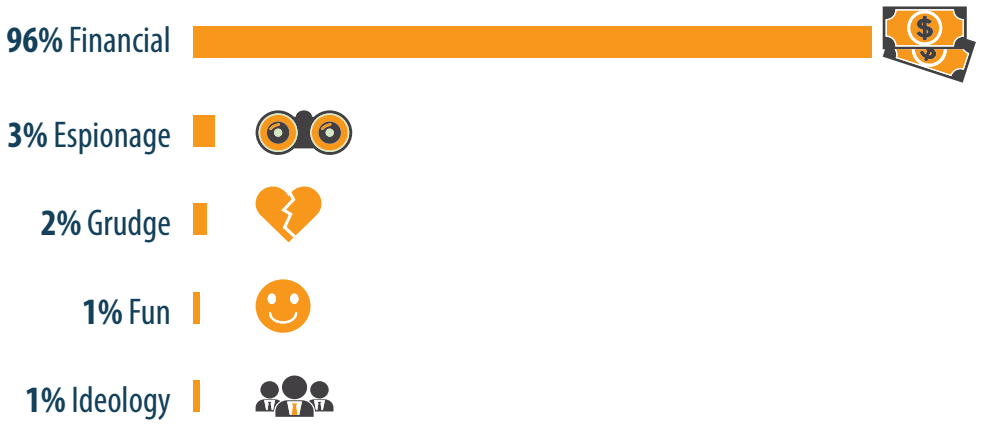
Counter IR can be disastrous for organizations. The best way to prevent an attack that compromises, steals, or deletes data is to strengthen cybersecurity measures altogether.

The average number of days to identify and contain a data breach is **287 days**.[1]

TAKE CONTROL OF CYBERSECURITY

Attacks are on the rise. As cyber criminals continue to make headway, Financial Institutions can improve resilience and decrease recovery times by implementing a comprehensive information security program.

Criminal motives for attacking the financial sector



2021 Data Breach Investigations Report, Verizon, 2021

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

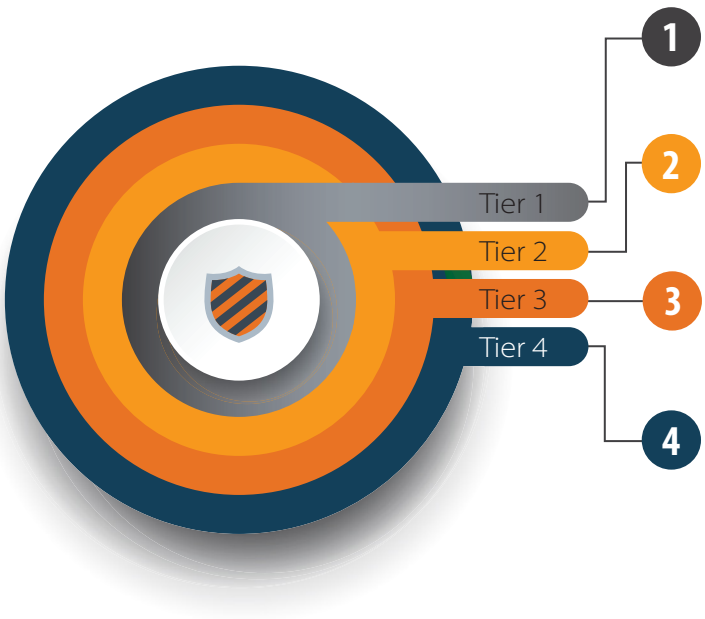
Customers expect their accounts to be secure, but they also crave technology solutions that give them more access to those accounts. Phase out legacy systems that predate current security requirements and eliminate overly complex manual processes to satisfy customers and thwart attackers.

A FRAMEWORK FOR CYBERSECURITY SUCCESS

In 2014, NIST released a voluntary, risk-based cybersecurity framework for critical infrastructure sectors. It 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



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

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

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

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

CSF Core Functions

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.

> Organizations that operate with fully deployed, mature security automation were able to identify and contain a data breach **77 days sooner**, or **27% more efficiently**, than those in early stages of maturation.[1]

IT'S A BUSINESS ISSUE, NOT AN IT ISSUE

As we all know, banks manage financial and credit risks— and 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 (e.g., 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.

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.

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.

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.

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.

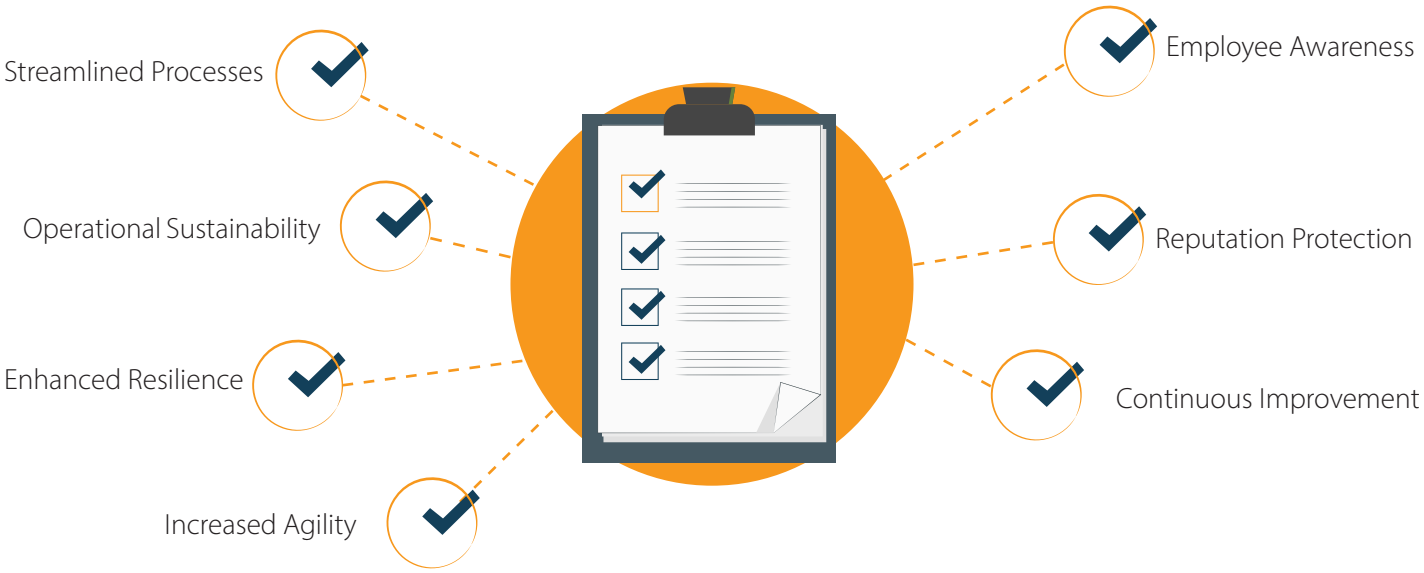
Information is power

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, 17 percent of data breaches are caused by miscellaneous internal errors.[3]

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



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.

If your business is ready to improve security and resilience, our consultants can help. Contact us 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. https://www.businesswire.com/news/home/20210428005365/en/COVID-Cyber-Crime-74-of-Financial-Institutions-Experience-Significant-Spike-in-Threats-Linked-To-COVID-19
2. https://www.ibm.com/security/data-breach
3. https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf
4. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists-2021.pdf

Agility and Stability: Developing Information Security Programs for Financial Institutions

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com