Next-level defenses for managing digital risks in financial services
Today’s world moves faster than ever before. Financial services companies recognize that they must match that pace – or risk being left behind.

However, they face a complex web of decisions in their digital transformation efforts. New technology platforms, outsourcing strategies, niche security products, and vendor relationships are everywhere.

Replacing everything is generally not an option. Financial services companies need their new solutions to work cohesively with existing infrastructure. Unfortunately, integrating new and legacy tools and systems adds complexity – and risk.

Managing that risk is more important than ever. Transformative services require you to take on risk, and often it isn’t in familiar categories like IT or legal. Cyber criminals have been innovating just as fast as the financial services companies they target. They are ready to seize onto any new vulnerability and rely on speed to beat your response.
In financial services, innovation cannot come at the cost of security or acceptable risk. Both are mission critical.

That’s why financial services companies need a risk management strategy that powers innovation while adapting to today’s threats.

In this eBook, we’ll answer three important questions about digital risks in financial services:

• What forces drive a need for digital sophistication?

• What is the weakest cybersecurity function in financial services?

• How can companies use more intelligent technology to better manage their vulnerabilities?

Then, we provide a framework for how financial services companies can overcome these risks and thrive in today’s changing world.

• In the last two years, 51% of financial services institutions (FSIs) have experienced a data breach.

• FSIs have seen an 18% increase in the volume of cyberattacks over the last 12 months, and a 27% increase in the severity.

Source: Ponemon Report
What forces drive the need for greater digital sophistication

There are four major forces driving a need for greater digital sophistication in financial services companies. How well companies adapt to these forces will impact their future success.

**Compliance and Regulation**
Data sharing and privacy regulations are changing how financial organizations conduct business across the globe. Whether it’s broadly scoped guidelines, as dictated by the EU’s revised Payment Services Directive (PSD2), or rules affecting a smaller region, as with California’s Consumer Privacy Act, organizations must comply with increasingly complex layers of regulation.

**Customer Expectations**
Customers have come to expect that financial organizations will be available to address their needs and concerns around the clock. This “always-on” and “real-time everything” environment demands the use of more sophisticated technologies, along with more advanced and automated protections to keep information secure.

**Data and Analytics**
Data lies at the heart of the industry’s transformation. Organizations are working to leverage data in new ways, make data more shareable, and mine it with more sophisticated analytics. In the EU, the U.K., and Australia – where financial institutions must adopt open banking – finding ways to securely share and manage data with third parties is a high priority. Shifts in data sharing raise new questions around both the security of data and who, ultimately, is accountable for managing and controlling the data.

**Cybercrime**
The frequency, severity and sophistication of cybercrime is rising, yet many data breaches still occur via well-tested approaches, such as phishing attacks. Those with criminal intent are closely following the industry’s transformation, looking for new points of entry and vulnerabilities. Financial organizations must be diligent about balancing investments in prevention, detection, and response. This keeps highly sensitive data secure and ensures the organization can respond efficiently if (or more likely when) there is an attack or breach.
Financial services organizations have dramatically increased their investments in security protections in recent years to defend against the growing sophistication of cybercrime. Security products generally fall under five primary categories aligned to the NIST Cybersecurity Framework: identifying threats, protecting against threats, detecting threats, responding to threats and recovering from threats.

Most organizations are heavily defended by products that help with the identification, protection, and detection of cyber threats. But responding to threats is still very much a patchwork process.

“On average, larger financial services organizations have at least 75 different products tackling different aspects of cybersecurity.”
What is the weakest cybersecurity function in financial services?

The weakest link in the framework today within financial services companies is responding to threats. To improve in this area, they must evolve past the current state.

Current State

Responding to cyber threats is still a highly manual process inside most financial services organizations, resulting in slow movement and errors at a highly precarious time. Security and IT tools are often disconnected, thwarting investigations and response. Analysts struggle to quickly assess the impact across the organization, which can take days of coordination between different people and teams, leaving critical systems vulnerable. Remediation involves ad hoc and firedrill processes between asset and data owners and security.

Desired State

Automating mundane, low-level tasks gets essential information quickly to the right people and directs human involvement only where it is truly required. Mobile experiences provide Security and IT professionals risk-aware visibility about vulnerabilities, attacks, and exposure across the organization, as they occur. Visibility comes with recommendations on steps to take, and “easy buttons” for taking action. Workflows direct resources to the right teams for immediate mitigation or severity-prioritized remediation. Throughout, people, process, and technology rise above functional boundaries to get the job done right, quickly.
A path forward for financial services: managing change and mitigating risk

Financial services organizations can’t afford to let anything interfere with their digital transformation. Instead, they must select the right tools and then empower employees to use those new technologies to take control, simplify processes, and accelerate progress.

Each of the four transformative forces can be managed – and turned into a competitive advantage – with the right approach.

**Compliance and Regulation**
Developing a centralized, integrated view of risk across the entire organization enables teams to reduce costs and findings and take quick action to resolve the most pressing compliance issues. Invisibly embedding risk and compliance activities into the front lines helps make risk practices more effective. Automating mundane compliance processes keeps talented employees focused on higher-level decisions and strategies.

**Customer Expectations**
The demand for real-time everything has financial services organizations testing new ways to become more customer-centric. But customers are not willing to accept tradeoffs between security, speed and responsiveness. To succeed in this climate, financial services organizations must do all of these.

**Data and Analytics**
Synthesizing business, asset, threat, and risk data provides critical context and detail to support rapid risk-based decision-making throughout the lifecycles of cybersecurity and risk management. Sharing that information across multiple parties in real time can have a dramatic impact on the business. As data is made more accessible, it is imperative to establish sound security protocols to rapidly assess, protect, and respond to security incidents — both inside the organization and with third-party vendors. Using artificial intelligence (AI) to sift through volumes of data at lightning speed can provide more meaningful insights for teams to act on.

**Risk Management**
Financial services organizations must be smart about how to use technology to fight the threats technology invites. Every second counts when it comes to a security incident — relying on manual processes leaves too much room for error and significantly delays response times. There are many ways to prevent reputational harm including: automating low-level tasks, contextualizing security and risk data with business insights, and employing a platform that connects all critical parties to develop an immediate, coordinated response to incidents.
How does ServiceNow help financial services companies manage risks and security incidents?

ServiceNow offers one platform, which works with legacy infrastructure as well as cloud, to provide an enterprise-wide view of security incidents, risks, and vulnerabilities. It also guides prioritization based on internal and external factors, and enable playbooks and workflows that automate and orchestrate the right responses.

• **Improve Vulnerability Response.** Create a comprehensive view of all vulnerabilities, connecting security and IT teams so organizations can respond faster.

• **Simplify Incident Response.** Flexible workflows and automation enable SOC teams to quickly prioritize and remediate incidents.

• **Improve Governance.** Develop an integrated view of risk to scope and prioritize security audits and automate mundane audit tasks.

• **Improve Compliance.** Streamline processes to work more efficiently.

• **Improve Risk Posture.** Manage risks both inside and outside of the organizations, with automated assessments of third-party vendors and risks.

A closer look: AMP takes security to the next level

AMP is an Australian-based financial services company offering superannuation, life insurance, investments, and advice.

The Challenge:
AMP largely managed its security vulnerabilities through manual processes and spreadsheets. They wanted to identify a quicker way to remediate security issues.

The Solution:
Automated ServiceNow processes mean teams now receive alerts about the context of an affected server or asset, along with the severity of the vulnerability, and its prioritization among issues happening across the entire organization.

The Results:
• 60% reduction in response time to general vulnerabilities; the reduction was even higher for critical issues
• 30% reduction in security incident response time
• 50% of configuration items were updated with correct IP information, improving the process

“ServiceNow has allowed AMP to process, prioritize, and action vulnerable systems. What used to take a roughly three weeks of manpower, has now been reduced to a single day.”

—Rahn Wakeley, Head of Cybersecurity, AMP Financial