deepwatch™

Bridging the Cybersecurity Skills Gap in Financial Services

Practical Staffing Strategies for Security Leaders

www.deepwatch.com

Table of **Contents**

Introduction

The financial industry is a primary target of cyber attacks due the lucrative nature of sensitive PII data, along with the frequency and speed at which that data is shared. Protecting these environments remains a challenge due to an expanding attack surface, a spike in cyber attacks due to geopolitical events, and attacks aimed to gain market strategies that can be used for insider trading[1].

Security leaders in banking, insurance, credit card, alternate payment networks and investment institutions must be particularly vigilant when it comes to protecting their organizations and their clients' data. Reputation, customer trust, investor confidence, regulatory penalties and revenue are all at stake.

Cyber insurance for financial services is also now more expensive and increasingly difficult to obtain. **Cyber insurance companies are mandating that their customers have certain security controls in place for insurability.**

Data breaches can severely impact a financial institution's bottom line. In 2021 the average **Total Cost of a Financial Industry Breach was $5.72M.**[2] The banking sector experienced a 1,318% year-on-year increase in ransomware attacks in the first half of 2021.[3]

Cybersecurity staffing shortages and skills gaps within teams make managing these risks difficult. Even well-funded security teams often cannot find or retain the advanced or specialized talent they need to protect the organization around the clock.

In this eBook, we provide actionable guidance to help make the case for an advanced security program with:

- **An improved security staffing process** that meets the needs of financial services SecOps personnel.
- **A fully optimized security operations center** that secures against threats in cloud, hybrid, and multi-cloud environments.
- **A risk management mechanism** to mitigate security risks associated with technology and staffing of security operations functions to secure the distributed enterprise and its data.

THE AVERAGE **TOTAL COST OF A FINANCIAL INDUSTRY BREACH WAS $5.72M.**[2]

Financial Security Staffing is a **Growing Risk**

Skills Gaps, Staffing Shortages, and Retention Issues

A recent study from (ISC)² revealed a critical finding: “Two-thirds of study participants report that a cybersecurity staffing shortage is placing their organizations at risk.”[4] This shortage is often referred to as the **cybersecurity skills gap**, and it means that in-house security teams often work extra hours and give up vacations and holidays[5] just to stay marginally on top of their workloads.

Staff turnover, high salaries, recruiting issues, and retention all contribute to this perfect storm. COVID-19 presented new opportunities to work from home which created even more competition in the market for technical talent.

According to ISACA’s new survey report, State of Cybersecurity 2022, sixty percent of those surveyed report difficulty retaining qualified cybersecurity professionals.[6] The long working hours and increasing threat pressures placed on IT security decision makers and teams are not sustainable at this pace.

Staffing an Advanced SOC

Financial institutions staffing a Security Operations Center (SOC) or fully integrating a SecOps program into the organization, will need a full complement of experienced staff available 24/7/365.

To operate efficiently and effectively, SOCs need the right people, processes, and technologies, such as up-to-date threat intelligence systems. They need to be staffed with enough analysts possessing the right capabilities and experience to evaluate what the tools and technology cannot.

Staffing a modern SOC can therefore be difficult. **There are currently over 115K unfilled/open finance sector cybersecurity jobs within the U.S.**[7] This short staffing increases organizational risk and can also cause burnout and possible churn.

An (ISC)^2 2021 study found that 60% of businesses surveyed said the lack of skilled cybersecurity professionals was putting their business at risk.

Despite progress in automation and the development of new monitoring technologies, every SOC still needs human intelligence, imagination, and insight to identify patterns and assess threat outliers that could indicate that an attack is underway.

60% OF BUSINESSES SURVEYED SAID THE LACK OF SKILLED CYBERSECURITY PROFESSIONALS WAS PUTTING THEIR BUSINESS AT RISK.

- ISC$_2$ STUDY

Alert Fatigue and Burnout

Alerts arrive from disparate security tools, each with a limited scope within the environment. These alerts on their own lack context. Unless there is a process to efficiently correlate and filter these raw alerts, analysts can be inundated with false positive alerts, making it extremely difficult for them to identify the threat. The result is alert fatigue, which can ultimately lead to burnout and distraction from real threats.

Meaningful alerts are created from a useful mix of curated playbooks, threat intelligence, IOC watchlists, machine learning, and automation. Such sophistication requires continuous adjustment and improvement in the alerting process.

Too Many Complex Security Tools to Manage

To cope with increased risk and the inability to find skilled staff, financial organizations often expand a SOC function by investing in security information and event monitoring (SIEM) solutions and intrusion detection systems (IDS). They often assume that automation and AI and ML can somewhat augment for a lack of qualified staff. **Advanced technology still can't fully compensate for the skills and expertise that an experienced cybersecurity professional can bring to SOC activities.** It's a burden on untrained staff trying to manage too many complex technologies which could risk turnover.

The addition of new technology can also serve to increase the burden on personnel. In the study "The Life and Times of Cybersecurity Professionals 2021,[8]" a cooperative research project by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA), **a third of the participants said that the skills shortage had created a scenario that prevented them from learning about or utilizing some of the company's security technologies to the fullest potential.**

Risk and Insurability

Operational disruption, material customer loss, and reputational damage are all business risks impacted by cybersecurity events. Businesses need to align security programs with their impact on business goals. However, in-house security may be too busy managing the status quo to have enough time to align business priorities, governance and compliance teams.

Compounding these risks are the rising costs related to cyber insurance. **The cyber insurance market has rapidly hardened with increased premiums and reduced coverage.** It also now requires security controls for different levels of protection or to receive any protection at all.[9]

Cybersecurity Compliance

As financial services try to cope with increasing cyber risk, governments and industries work to create cybersecurity and data policy to protect both organizations and their customer data. Banks are now required to notify regulators within the first 36 hours after an organization suffers a qualifying "computer-security incident.[9]

The increasing number of complex regulations and the risk of non-compliance fines puts pressure on enterprises to hire knowledgeable staff to facilitate security compliance and risks management concerns.

The current staffing shortage makes it difficult for maturing institutions to adequately address regulatory, risk, and compliance concerns. Financial SOCs must be staffed with individuals skilled in compliance framework and risk management processes unique to the financial services industry.

Bridging the Skills Gap in **SecOps**

The bridge to improved security operations can be built in a number of ways.

Financial organizations today can choose from one of the following three options:

- **Hire an in-house Security Operations team** and build an in-house Security Operations Center.
- **Hire an in-house team to work with a Managed Security Services Provider (MSSP)** for basic security service support.
- **Partner with an expert-led Managed Detection and Response (MDR)** provider for fully managed, outsourced 24/7/365 Security Operations experts and technology services.

According to a recent survey by Deepwatch, **38% of surveyed financial companies indicated that they would invest in managed services** to address their shortage of qualified security staff.[7]

Many banks, insurance companies, credit card companies and other institutions do not have the resources necessary to build a modern SOC infrastructure and staff the full bench of security professionals they need to succinctly manage their unique security risks. Deepwatch survey also found that companies 24x7x7365 SOC are more likely to respond to security threats faster.[7]

MDR providers offer a variety of tools and services, but their offerings can vary widely. When a real-time incident occurs, real-time response may be limited to billable customer service hours conducted by off-shore call centers, while escalated security alerts may offer little to no context for the in-house team's investigation or documentation.

The option to partner with a **US-based, expert-led Managed Detection and Response provider** delivers added value and provides cybersecurity at scale. With the right MDR provider, hard-to-hire experts provide eyes-on-glass around the clock to ensure anomalies in their customer's security environment are detected quickly.

If a true threat is identified, security specialists immediately contact the customer to coordinate rapid response activities to stop the threat fast and minimize financial impacts. **With MXDR capabilities, outsourced teams can enable XDR outcomes: high-fidelity alerting, extended detection of threats across on-prem, cloud and SaaS and precision response across the distributed enterprise.**

Benefits of Using MDR to Staff Your SecOps and SOC

Working with the right Managed Detection and Response (MDR) provider can help financial services organizations to optimize the entirety of their security operations. **Outsourcing SecOps and SOC** activities to an MDR offers cost-effective benefits over attempting to manage security in house.

Working with an MDR provider to deliver security services can help:

- **Reduce Cybersecurity Costs** – Whether an organization is developing their overall security processes or wishing to build and maintain a SOC, these activities can be expensive—both in terms of staff and technology. An MDR provider can offer the expertise and latest technology solutions, getting the most value for your spending and demonstrate a successful ROI.
- **Reduce Alert Fatigue** – Through a combination of curated threat intel and advance correlation, the right MDR can reduce the burden on existing staff and allow them to focus on other important initiatives.
- **Save time spent on false positives –** When the wrong provider sends over too many false positives, this time spent can be a waste in time and company resources.
- **Support Compliance Readiness –** Support regulatory compliance by identifying and prioritizing most critical vulnerabilities.
- **Inventory Management** – An MDR provider can help SecOps and SOC teams inventory all endpoints and users on a network.
- **Ongoing Management and Maintenance of Security Tools –** SOCs require quite a few advanced technology tools—sometimes more than 20. MDR staff can support financial businesses by helping determine which tools to purchase, facilitating the purchasing process, and installing the technologies, then managing and maintaining the tools.
- **Incident Response** – An optimized SOC operates 24/7/365. An MDR provider can offer the SOC staff the support necessary to ensure no alert, anomaly, incident, or attack gets missed, particularly on holidays, weekends, or at night.
- **Improve Visibility –** MDR partners have the staff to provide 24/7/365 monitoring with the skill sets to analyze and correlate attacks across millions of transactions. Staff also possess the unique skills needed to identify sophisticated attacks during threat hunting activities.
- **Improve ROI** – MDR providers can help leverage existing technology solutions to improve ROI by maximizing the value of your existing tools.
- **Seamless integration –** MDR providers have the experience and expertise to integrate operations, staff, and additional technology solutions seamlessly with existing enterprise SEIM, vulnerability management, and active response.

The Right MDR Provider Can Support Both SecOps and SOC Activities

An experienced and customer focused MDR partner can support SecOps and SOC efforts by providing:

- **High-touch Delivery model** that embeds resources within the customer organization and serves as an extension of the security teams
- **24/7/365 monitoring of the environment by US-based experts** with a broad range of skills, knowledge, and experience
- **Advanced threat detection** of threat behaviors with indicators of attack
- **The right SIEM technology** to collect massive volumes of data in real-time, detect advanced attacks, and raise alerts about anomalies such as insider threats and other hard-to-detect use cases
- **Decreased alert noise** with advanced correlation and threat analytics
- Integrated endpoint detection and response **(EDR) that can help meet cyber insurance requirements**
- **Firewall (FW) management** for managing and monitoring firewall deployments in order to protect network traffic and prevent unauthorized access
- **Risk management strategies** to help improve the security posture on a continuous basis
- Access to comprehensive **Content Library of use cases**
- **Proactive hunting** for indicators of compromise to identify attackers
- Capabilities to notify stakeholders to isolate affected endpoints and network segments to **contain threats and roll back any unauthorized changes with expert guidance**

Security Operations **Staffing for the Future**

The long working hours and increasing threat pressures placed on IT security decision makers and teams is not sustainable. Security leaders must fund resources that best maximize security investments and outcomes. Most importantly, they must secure and protect systems from operational disruption that could expose sensitive PII data.

To cope with both staffing and budget challenges, **the most efficient and cost-effective way to manage the increasing proliferation of threats** and attacks is through a fully functioning and expert staffed SecOps team and SOC that has the built-in capability to scale for both business growth and evolving threats.

A trusted **Managed Detection and Response** provider helps organizations maximize investments and advance security team maturity. With an expert staff for 24/7/365 threat detection and incident response, organizations maintain business continuity in the short-term, advance security maturity over time, and increase their security posture to prepare for future threats.

SOURCES

1. Modern Bank heists 5.0: The escalation from dwell to destruction. VMware News and Stories: *https://news.vmware.com/security/modern-bank-heists-5-0-the-escalation-from-dwell-to-destruction*
2. 2021 Cost of a Data Breach Report, IBM: *https://www.ibm.com/security/data-breach*
3. Trend Micro: Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats: *https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats*
4. (ISC)^2 Cybersecurity Workforce Study, 2021: *https://www.isc2.org/Research/Workforce-Study*
5. Overworked CISOs are skipping family vacations and holidays. Infosecurity Magazine: *https://www.infosecurity-magazine.com/news/overworked-cisos-are-skipping/*
6. State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyber operations, ISACA: *https://www.isaca.org/go/state-of-cybersecurity-2022*
7. State of the Modern SOC Survey by Deepwatch 2022
8. ESG RESEARCH REPORT, The Life and Times of Cybersecurity Professionals 2021, Volume V, A Cooperative Research Project by ESG and ISSA: *https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf*
9. Gallagher, Cyber Market Conditions, January 2022: *https://www.ajg.com/us/news-and-insights/2022/jan/2022-cyber-insurance-market-report/*

About Deepwatch's Managed Detection & Response Services

Deepwatch is a trusted security leader, offering professional and innovative managed security to help support security operations to stop breaches and attacks. Deepwatch's managed detection and response services include 24/7/365 threat monitoring, alerting, validation, and proactive threat hunting, with accelerated detection of malware, botnets, and ransomware behavior.

At Deepwatch, organizations work with Deepwatch experts, including detection and response analysts and threat hunters who take time to understand a business's unique environment.

Deepwatch customers have experienced greater than 430% ROI on their MDR investment with over 98% reduction in false positives enabling them to focus on strategic initiatives. Moreover, through real-time collaboration and engineering refinements, customers' environments have seen 40%+ improvements in security maturity every year.

deepwatch™

ABOUT DEEPWATCH

Deepwatch® is the leading managed security platform for the cyber resilient enterprise. The Deepwatch Managed Security Platform and security experts provide enterprises with 24x7x365 cyber resilience, rapid detections, high fidelity alerts, reduced false positives, and automated actions. We operate as an extension of cybersecurity teams by delivering unrivaled security expertise, unparalleled visibility across your attack surface, precision response to threats, and the best return on your security investments. The Deepwatch Managed Security Platform is trusted by many of the world's leading brands to improve their security posture, cyber resilience, and peace of mind. Learn more at www.deepwatch.com

Visit www.deepwatch.com or reach out to us at sales@deepwatch.com

CONTACT US

4030 W Boy Scout Blvd, Suite 550
Tampa, FL 33607
(855) 303-3033