Point of View

Build Your Own Security Operations Center or Partner With a Managed Security Service Provider?

The financial risks from ransomware are substantial. Lost revenues, lost productivity and recovery costs can add up to millions. Repairing customer and partner relationships, rebuilding brand, as well as legal and contractual mitigation are costly. According to Ponemon, the average cost of a cyberattack exceeds $3 million.

Contrary to the beliefs of many, small-to-medium businesses (SMBs) are top targets for cybercriminals.

Verizon's most recent Data Breach Investigation Report (DBIR) determined that 43 percent of all data breaches targeted SMBs. Why? Most SMBs are underprotected and hackers know it. Underprotected companies offer the path of least resistance and the quickest return on investment for a cyberattack. Regardless of company size, however, the financial risks demand an effective, efficient and high-end security operations center (SOC) to protect their businesses.

Today's attacks are sophisticated, fast moving and evolving.

Today's SOC needs to be equally sophisticated, fast moving and evolving.

Cybercriminals continuously develop new attack vectors with a specific focus to evade endpoint protection solutions. According to AV Test, in 2018, 137 million new malware variants were released. Threat actors continuously evolve living-off-the-land and obfuscation techniques that NextGen AV and EDR fail to detect.

In this treacherous environment, organizations need to dramatically improve their security posture. Executive management must weigh the costs/benefits of building, staffing and managing their own SOC, or partnering with a managed security service provider (MSSP). When making this decision, it is important to understand that cybersecurity is hard and expensive.

There are three considerations in this "build" versus "buy" decision:

- SOC staffing costs
- Security infrastructure costs
- Time to maturity

SOC Staffing

Cybercrime is global. With increasing threats coming from China, Russia and elsewhere in the world, it's always nine to five somewhere. As a result, a SOC needs to be staffed for 24/7/365 operations. The size of a SOC does not have a linear relationship to the size of the company. Instead, you should think about critical mass. For optimal protection, a SOC should be organized into four shifts.

Shifts should have some overlap to ensure an efficient transfer of information, but also to cut down on the number of shift changes. Staffing must also account for vacation and sick time. At a minimum you will require five to six security analysts for round-the-clock protection. Twelve analysts would be optimal.

A senior research analyst will play an important role in securing your environment. They sift through threat intelligence feeds to identify new and emerging attacks that pose a threat to your organization. They work closely with security analysts to proactively prepare them to detect and mitigate these new threats.

Lastly, you'll need director-level personnel with the experience and vision to lead the team.

With CyberProtect℠ from Fiserv, you get the best. We have analysts whose experience goes beyond the garden variety threats. We look for analysts who have gone up against the most sophisticated state-sponsored and organized crime. We look for specific character traits: passion for security, insatiable curiosity and a tenacious desire to win. Finding, hiring and keeping these experts in today's market is difficult.

The U.S. Department of Commerce estimates there are over 350,000 unfilled security positions in the United States. So, it's a job seeker's market.

Don't forget hiring costs. Recruitment fees average between 15 – 25 percent of the first year's pay.

Anticipated/Expected Salaries:

• Security Analyst	$90,000 to $150,000
• Research Analyst	$125,000 to $165,000
• Director/Team Lead	$150,000 to $180,000

Security Infrastructure Costs

Hiring your SOC team is the first step. The second step is providing them with the tools to convict, contain and mitigate threats efficiently and effectively. Threat detection solutions, such as NextGen AV, Endpoint Detection and Response and log capture, are staple security technologies. However, faster and more effective response to detected threats relies on other security technologies.

It's all about enabling and empowering the analysts. Security information and event management (SIEM) correlation across network and endpoint data sources and threat Intelligence enriches threat data for faster and more accurate conviction and mitigation. Security Orchestration Automation and Response (SOAR) automates security operations while automatically collecting contextual evidence. It allows analysts to spend more time in investigation and less time collecting data.

Time to Maturity

Set-up and ramp-up of a new SOC takes time. Security systems and their agents need to be installed. NextGen AV and EDR policies need to be tuned. SOAR playbooks need to be customized. Threat Intelligence Platforms need to be built. And, security analysts need to be hired and onboarded.

In all, it takes about six months to get a SOC up and running. It takes about twelve to eighteen months for a new SOC to reach maturity and deliver optimized protection. In the meantime, your IT assets and business operations remain exposed to attack.

The chart below summarizes SOC staffing costs, security infrastructure costs and time to maturity for an organization with 1,000 endpoints. The annual costs in this example add up to a little over $1.2 million.

One time hiring costs total $194,000. And as stated above, you should plan on six months to get up and running and twelve to eighteen months to reach maturity.

	Annual SOC Staffing	**Hiring Costs**
Six SOC Analysts	$660,000	$132,000
One Research Analyst	$145,000	$29,000
One Director/Team Lead	$165,000	$33,000
Total	**$970,000**	**$194,000**

Security Infrastructure	**Annual Subscription**	**Ramp-up Time (Days)**
NextGen AV	$22,580	15–20
SIEM	$15,000	60–90
Vulnerability Management	$15,360	30–60
AWS	$30,000	15–20
Threat Intelligence Feeds	$100,000	30–60
SOAR Platform	$50,000	60–90
Total	**$232,940**	**Up and running: 6 months** **Maturity: 12–18 months**

*Assumption: Cloud-based subscription prices

**Estimated costs may vary by vendor and client infrastructure

The Advantages of Partnering with an MSSP

A sophisticated, fast-moving and evolving MSSP excels at detecting, containing and mitigating threats. MSSPs deal with these threats all the time. Fiserv invests significant money and resources on advanced detection and response techniques – freeing up our clients to spend more time managing their business. Partnering with an MSSP like Fiserv will cost less than 25 percent of the annual costs of building an in-house SOC. MSSP clients also benefit from payroll savings associated with security and research analysts. And, they save on hiring costs.

Clients still pay a per-sensor price for endpoint security solutions (NextGen AV and/or EDR). However, they save on the annual costs associated with a SIEM platform, SOAR platform and threat intelligence feeds. Partnering with an MSSP spreads these costs across multiple clients.

And perhaps the most important MSSP advantage, clients immediately benefit from the protection delivered by a mature SOC. An experienced MSSP like Fiserv can ramp up a new client within a week. This eliminates an extended security risk while trying to ramp up an in-house SOC. Also, with experienced MSSPs such as Fiserv, the knowledge gained across an entire client base serves to enhance the protection an MSSP delivers to all its clients.

About the Authors

Professional Experience Summary

Nayan Patel is responsible for finding best of breed technology partners and solutions to enable Fiserv clients to secure their technology environment and focus on their core business. Nayan currently leads the Fiserv alliance with BlueVoyant, which offers a comprehensive, state-of-the-art cybersecurity solution designed specifically for financial institutions. He spent the previous 15 years running technology organizations in the Financial Solutions space. Prior to taking on his current role, Nayan was Vice President, Data Center Operations at Fiserv responsible for providing Core and Digital services to over 500 Banks and Credit Unions in Data Centers located across the United States and Canada. In this role Nayan was responsible for providing platform availability, performance, scalability, compliance and overall data security to over 10 million consumers of Financial Services technology.

Nayan Patel, Vice President
Cybersecurity Practice
Fiserv

About the Authors

Professional Experience Summary

Travis Mercier is the Head of Global Security Operations for BlueVoyant, responsible for the day to day operations of BlueVoyant's Global Security Operations Centers and Threat Fusion Cell.

Travis has 13+ years of experience concentrated in Information Technology, Cyber Security Operations and Cyber Defense Centers, Incident Response, Security Monitoring, Cyber Hunting, Digital Forensics and Cyber Threat Management.

Prior to joining BlueVoyant, Travis lead the Customer Security Operations Center (CSOC) and the Managed Security Threat Intelligence Cell for Rackspace Managed Security. Travis has built, led and operated SOCs for seven organizations, five of which are Fortune 500 organizations. Travis has also led and performed large scale incident response for multiple high-profile data breaches involving sophisticated adversaries and nation-state level threats. Travis was previously a Senior Consultant at CrowdStrike and a Senior Consultant at Ernst and Young (EY).

Travis Mercier, CISSP
Head of Global
Security Operations
BlueVoyant

Connect With Us

For more information about managed security services from Fiserv, call 800-872-7882, email getsolutions@fiserv.com or visit fiserv.com.

Fiserv is driving innovation in Payments, Processing Services, Risk and Compliance, Customer and Channel Management and Insights and Optimising. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today. Visit fiserv.com to learn more.

fiserv.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
fiserv.com

558963 03/20