

HOW MUCH DOES IT REALLY COST TO MANAGE CYBERSECURITY?



MANAGED SECURITY SERVICES PROVIDER

vs.

IN-HOUSE CYBERSECURITY

TOTAL COST / YEAR \$24,000-\$90,000*

Expect less than the cost of 1 in-house cybersecurity professional at a flat, monthly rate. Services are all-inclusive and operate 24x7.

Additionally, an MSSP will shoulder the cost of infrastructure and storage.

**Please note that pricing will vary; this is an example of an average cost for a Small to Medium-sized business (SMB).*

TOTAL COST / YEAR \$400,000+

Expect a high cost for talent, with massively increased overhead; slow adoption of new technologies and slow reaction to new risks.

For the cost comparison below, we define a Small to Medium-sized business (SMB) to have 500 employees with 3 or less locations and no more than 1,000 endpoints.

LET'S BREAK IT DOWN

TECHNOLOGY COSTS Included

HARDWARE, SOFTWARE, INFRASTRUCTURE, & SUPPORT

Partnering with an MSSP allows organizations to not only adapt cybersecurity for their growing business by providing it with the expertise, infrastructure, and storage but will also continuously ensure technologies and processes are kept up-to-date with the evolving threat landscape.

An MSSP operates on a SOC-as-a-Service model, meaning all sensors, servers, storage, technologies, and applications are included at a fraction of the cost of having them in-house.

TECHNOLOGY COSTS \$ 100,000+

HARDWARE, SOFTWARE, INFRASTRUCTURE, & SUPPORT

For organizations attempting to build their own Security Operations Center (SOC), they can expect two major associated costs: the cost of acquiring cybersecurity technology and the cost of hosting cybersecurity technology. A SOC will host a SIEM, which is the most common hardware needed to sustain security in an environment. Working alongside the SIEM are technologies such as firewalls, advanced threat detection (ATD), vulnerability management (VM), network access control (NAC), mobile device management (MDM), and an Intrusion Detection System (IDS).



Additional benefits include:

- Comprehensive threat detection and actionable incident response directives
- Out-of-the-box compliance reporting
- Holistic Security Architecture
- Integrated Threat Intelligence
- Lifecycle management of the SIEM
- Extensive training for your employees to learn how to avoid attacks

To start, building a SOC will cost anywhere between \$188,000-\$269,000:

	SIEM: \$25,000-\$40,000
	VM: \$10,000-\$20,000
	IDS: \$10,000-\$30,000
Network Behavior Analytics Detection:	\$10,000-\$15,000
External Threat Intelligence:	\$20,000-\$100,000
Orchestration & Collaboration:	\$15,000-\$75,000
Ticketing & Reporting:	\$5,000-\$25,000

SERVICES COSTS

 **Included**

CORE CAPABILITIES

As cyberattacks become more sophisticated, organizations know it is imperative to have and maintain a strong security posture. However, organizations may lack adequate security intelligence on staff. Additionally, dedicating someone 24x7 can be a challenge for an already busy IT department. Lastly, budgeting for security products and stand-alone services is not efficient. An MSSP can solve many of these problems.



ASSET DISCOVERY

The first step to securing an environment is to obtain a thorough understanding of what is on an organization's network:

- Passive Network Discovery
- Active Network Scanning
- Asset Inventory
- Host-based Software Inventory



VULNERABILITY ASSESSMENTS

An MSSP uses active network vulnerability scanning techniques to identify specific operating systems and services running on assets, as well as versions of software installed and their patches:

- Continuous Vulnerability Monitoring
- Attack Vector/Avenue Identification
- Continuous Compliance Monitoring

SERVICES COSTS

 **\$100K-\$150K +**

CORE CAPABILITIES

Most organizations will need to find a solution or suite of technologies that are tailored specifically to their needs. Top things to consider are the size, industry, risk appetite, cybersecurity posture, the organization's need for compliance and last but not least, the available IT budget. Aside from these considerations, organizations will likely assume 100% liability in all incidents that occur.



ASSET DISCOVERY

Asset Discovery has different meanings to different IT admins. To some, it's asset management. For others, asset lifecycle tracking using bar code scanners is asset management. Asset Management software varies in cost based on how its delivered.

Cost to an SMB: \$15,000 / year



VULNERABILITY ASSESSMENTS

With network vulnerability assessments, weak spots in an organization's critical assets can be identified. Automated vulnerability assessment scans run automatically at regular intervals so manual scanning routine isn't completed manually. This keeps false positives from occurring through normal human review, and allows real prioritization of the findings.

Cost to an SMB: \$4000 / year and \$10,000-\$25,000 for ongoing assessment and consulting services.



SERVICES COSTS

Included



THREAT DETECTION

An MSSP performs advanced threat detection across your cloud, on-premises, and hybrid environments:

- Network Intrusion Detection (NIDS)
- EndPoint Detection and Response (EDR)
- File Integrity Monitoring (FIM)
- Thousands of Correlation Directives & Rules
- Hundreds of Threat Intel Data Feeds



BEHAVIORAL MONITORING

Behavioral monitoring for a network, its systems, and users is essential for spotting threats and can be useful in investigating suspicious behavior and policy violations:

- Real-time Service & Infrastructure Monitoring
- Netflow Analysis
- Network Protocol Analysis
- User Activity Monitoring



HUMAN BEHAVIOR SECURITY ASSESSMENT

Humans are our most important assets and risks should be calculated based on how susceptible a user is to a compromise within the environment. An MSSP provides fully managed testing, analysis, and reporting on employee responses to simulated phishing attacks in order to reinforce security awareness through "teachable moments":

- Simulated Phishing Attacks
- Results correlation with threat detection capabilities



SECURITY INTELLIGENCE

Effective security intelligence provides the information necessary to detect threats and subsequently contain them by defining security intelligence as the technology and processes used to detect compromises and coordinate the appropriate responses:

- Security Incident & Event Monitoring (SIEM)
- Log Management
- Security Event Correlation
- Incident Response
- Threat Intelligence

SERVICES COSTS

\$100K-\$150K +



THREAT DETECTION

Threat Detection utilizes big data analytics to find threats across large and disparate data sets, which often includes crowdsourcing across the Internet. The objective is to find anomalies, analyze their threat level, and determine what action may be required in response.

Cost to an SMB: \$20,000 - \$100,000



BEHAVIORAL MONITORING

A Behavioral Monitoring solution will likely monitor users activity across networks, servers, storage systems, and databases. Training an organization's employees, ensuring that the software integrates well in the environment, and expecting customization across dashboards are usually additional services.

Cost to an SMB: \$10,000 - \$30,000



HUMAN BEHAVIOR SECURITY ASSESSMENT

As users are generally the last line of defense for most organizations, it's imperative that they are trained in recognizing phishing campaigns and other attacks.

Organizations attempting to do this in-house may use tools that are free or low-cost, but these won't likely provide in-depth and ongoing training over time.

Cost to an SMB for 500 employees: \$10,000 / year



SECURITY INTELLIGENCE

Turning security intelligence data from multiple sources into actionable, contextual information can be challenging for many organizations approaching it on their own. Most vendors work on a subscription model, providing data feeds, alerts and reports.

Cost to an SMB: \$15,000-\$75,000 / year



SERVICES COSTS

\$ Included

PERSONNEL

One of the most sought after benefits of partnering with an MSSP is the expertise and experience its talent can bring to an organization both from a technical perspective and an industry-specific perspective. An MSSP team may look like this:



TRAINING

An MSSP will keep its employees' certifications up-to-date by providing ongoing training annually alongside growth opportunities. Additionally, a shared resources model will help ensure that talent is cross-trained in different industries and technologies. This is very helpful in situations when a staff member leaves, as that person will not be the only one with the expertise needed to keep operations running efficiently for customers.

An organization can expect a team of engineers from an MSSP to have the following certifications and training:

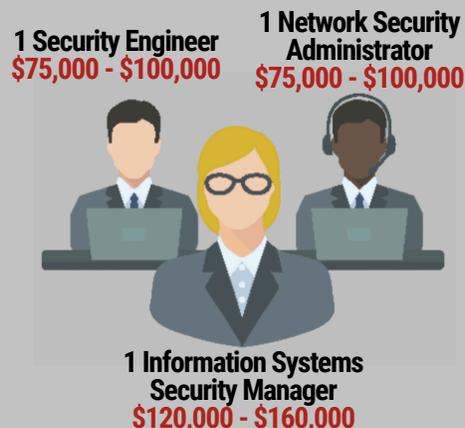
- CompTIA's Security + (Sec +)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Global Information Assurance Certified (GIAC)
- Intrusion Analyst
- Offensive Security Certified Professional (OSCP)

SERVICES COSTS

\$ \$400k+

PERSONNEL

Many enterprises may consider implementing a 24x7 Security Operations Center (SOC), which is considered a best practice. A SOC will require hiring somewhere between 5 and 20 security engineers with vast experience. Here's what an organization's internal staff team may look like:



TRAINING

As the threat landscape continues to move at the sound of speed, organizations must ensure that their engineers and analysts are current on necessary certifications - which excludes the training course and renewal fees. Here is an approximate breakdown of the recommended certifications with associated costs*:

Sec +
 Training Cost: \$3,504
 Exam Fee: \$320
 Renewal Fee: \$50

CEH
 Training Cost: \$5,200
 Exam Fee: \$500
 Renewal Fee: \$80

CISSP
 Training Cost: \$3,100
 Exam Fee: \$699
 Renewal Fee: \$85

CISM
 Training Cost: \$5,194
 Exam Fee: \$465-\$595
 Renewal Fee: \$45-\$80

GIAC Intrusion
 Training Cost: \$6,210
 Exam Fee: \$729
 Renewal Fee: \$429

OSCP
 Training Cost: Lab included in exam fee
 Exam Fee: \$729
 Renewal Fee: \$429

If an organization has a similar staff to the one we've illustrated above, we will assume each staff member will need training for each exam as well as 1 renewal per year for each certification. After totaling all certification costs, it'll cost an organization approximately \$27,993 per person per year, or \$83,799 in training expense alone for a staff of just 3 people.

THE COST OF A DATA BREACH

The Verizon Data Breach Report defines a Data Breach as "an incident that results in the confirmed disclosure not just potential exposure of data to an unauthorized party. While industry and location influence the cost of a data breach to an SMB, the following factors are true cost determinators:

01 COST OF BREACH BY CUSTOMER CHURN

Small to Medium-Sized Businesses with a churn rate less than 1% experienced a **\$2.6M** cost to the business according to the Ponemon Institute*



COST OF BREACH BY NUMBER OF LOST RECORDS

02

The more records lost, the higher the cost of data breach. In 2017, the cost ranged from **\$1.9M** for incidents with less than 10,000 compromised records to **\$6.3M** for incidents with more than 50,000 compromised records*

03 COST OF BREACH BY TIME TO IDENTIFY AND CONTAIN BREACH

On average in 2017, the mean time to detect a breach was 190 days and 66 days to respond to a data breach. The cost of a breach going undetected for 190 days is over **\$3M**, with the cost of not responding to a breach in under days costing **\$3.77M***



COST OF BREACH BY ESCALATION AND DETECTION

04

Detection and escalation costs include forensic and investigative activities, audit and assessment services, as well as crisis team management. In 2017, the average escalation and detection cost for companies in the U.S. was **\$1.06M***

05 POST- DATA BREACH COSTS

Ex post costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. In the U.S., costs were **\$1.56M** for SMBs



HOW AN MSSP CAN HELP



GREATER SECURITY COMPETENCY

Security Monitoring, Event Correlation and Alerting, Intrusion Detection System, SIEM, Firewall and Threat Intelligence are all included services when partnering with an MSSP. Additionally, an MSSP will likely be well-versed in mitigating issues and providing protection and recommendations for an organization on a security strategy.

IMPROVED REGULATORY COMPLIANCE

As regulatory environments continue to evolve, it becomes critical that an organization monitors compliance levels across regulations such as GDPR, PCI DSS, DFARS, SOX, HIPAA, FISMA, ISO and others. An MSSP brings expertise in both processes for becoming compliant, and further maintaining it.



REDUCED COST AND OVERHEAD

As we've concluded, an MSSP is much more cost-efficient than building and managing an in-house cybersecurity team. Cost aside though, an MSSP team will be available 24x7x365 and will always be up-to-date in certifications needed to ensure a strong security posture for an organization.

AUGMENTED SKILLSETS AND EXPERTISE

According to Cybersecurity Ventures, it's estimated that there are currently 350,000 open cybersecurity positions in the US, and a predicted global shortfall of 3.5 million cybersecurity jobs by 2021. This will make it even harder for organizations who plan on staffing their own cybersecurity teams to do so in the future. Not only do MSSPs keep their security engineers and analysts trained and certified, but they will likely have both private and public sector experience.



MAD SECURITY

MAD Security is a leading provider of advanced information and cybersecurity solutions, offering a seamless blend of technology, expert services, dedicated support, and comprehensive training. With a proven track record across diverse industries, MAD Security empowers organizations to effectively manage risks, achieve regulatory compliance, and lower costs through its innovative managed security services model.

Committed to delivering cybersecurity excellence, MAD Security provides tailored solutions designed to optimize security performance, enhance operational efficiency, and protect against evolving cyber threats.

