



THE 5 PROVEN BENEFITS OF A MANAGED SECURITY SERVICES PROVIDER (MSSP)



A hand in a white shirt pointing towards a red hexagon containing the text 'CYBER SECURITY'. Below it is a grey hexagon containing 'INFORMATION PRIVACY'. The background is a blurred image of a person in a white shirt. There are also faint, semi-transparent text elements like 'NETWORK SECURITY' and 'ATION' visible in the background.

CYBER SECURITY

INFORMATION PRIVACY

WE'RE AT THE TIPPING POINT FOR BUSINESSES AND CYBERCRIME.

Despite massive breaches involving government entities and businesses across industries and geographies, the cost to organizations themselves didn't appear significant – until now.

In 2017, cyber attackers compromised more than 1 billion accounts and records, according to Gartner. Cybercrime costs will reach \$2 trillion by 2019, and cybersecurity spending will reach \$1 trillion in 2018.

We won't focus on the much debated statistic claiming 60 percent of all small business are out of business six months after a breach, which was discussed in Congress. However, a Ponemon Institute survey found that **55 percent of small and mid-sized businesses reported experiencing a cyberattack within the past 12 months, and only 14 percent considered their security defenses to be highly effective.**

It's difficult for many businesses to maintain sufficient cybersecurity capabilities. A solution that has empowered many security teams is to partner with a managed security services provider (MSSP) to secure critical assets and data.

MANAGED SECURITY SERVICE PROVIDERS

Services to identify and minimize business risk

24x7x365 protection against threats

Empowering security teams with the people, processes and technology to bolster security maturity

MSSPs can deliver the latest and most advanced capabilities, 24/7 availability and dedicated analysts. Meanwhile, businesses avoid the large capital and operational expenditure of maintaining their own capabilities and programs.

In a recent survey of 301 U.S. IT security professionals

87%

reported planning to migrate to a security-as-a-service model within the next year.



Another recent survey reported

86%

of IT security professionals either already partner or plan to partner with an MSSP.



There are five critical reasons why MSSPs are the growing solution to the challenging and demanding requirements businesses face when it comes to securing their assets and data.




SUPERIOR PROTECTION

When your security tools generate billions of actions per month – with less than one in 1 million signaling legitimate threats – the majority of analysts are likely to ignore most threats altogether. The overwhelming number of false positives hinder organizations' ability to protect themselves.

THE ALERT FATIGUE PROBLEM

Security research shows:

▶ **31%** 
of respondents ignore alerts because so many are false positives

▶ **40%** 
feel the alerts they receive lack actionable intelligence

(source)

To combat alert fatigue, internal teams often buy multiple cybersecurity solutions. However, the multitude of silos they create by doing so exacerbates the problem. The solutions don't work together seamlessly, and the different logs, alerts and data they generate can be impossible to analyze in a meaningful way, thus creating additional security events.

By contrast, MSSPs can build layered solutions with advanced security technologies tested across multiple enterprises. From vulnerability assessments to penetration testing to overall security program review and development, MSSPs build resilient defensive programs that are difficult for the vast majority organizations to construct themselves.

2

COST SAVINGS

Modern cybersecurity programs are costly to assemble and maintain. The tools and capabilities mentioned previously often require dedicated hardware or appliances, and frequently come with annual licensing costs. In addition, staff salaries and training to use the new tools add to the price.

For example, a business might need to establish 24/7 monitoring capability. Up-front investment requirements would include security information and event management (SIEM) solutions and other cyber technologies, software licenses, staff training, and staff salaries for the multiple specialists required to monitor a solution around the clock. For a fraction of the cost, the business could partner with an MSSP and get 24/7 coverage.


This is no small issue. Cybersecurity salaries are rising at almost 7 percent annually and frequently start above \$100,000. Meanwhile, the field is expected to have more than 1.5 million unfilled positions by 2020. The cost of acquiring and retaining talent amid these conditions is onerous for individual organizations, but MSSPs can distribute the expense of a shared service across broad client bases. MSSPs provide smaller companies with access to expertise and technology that would be prohibitively expensive to build in-house.

SURVEY SAYS: SAVINGS

In one Forrester research report, migration to a network security MSSP provided an ROI of

▶ **152%** 
with a total cost savings of
\$1.3 MILLION over three years

A study by CompTIA reported that

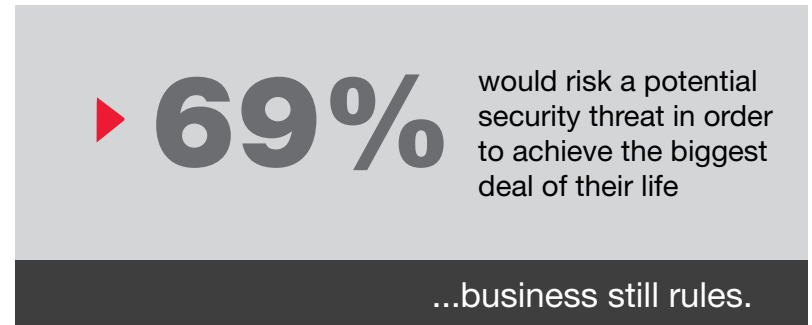
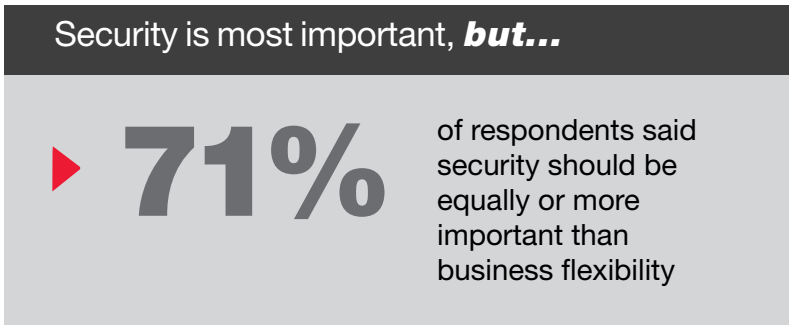
▶ **46%** of managed IT service users have cut their annual IT costs by
25% or more by outsourcing to MSSPs. 

3

BUSINESS FOCUS

Information security needs to support the mission of the organization and should mitigate, transfer or accept risk in order to evaluate overall business risk. Too often, cybersecurity professionals get wrapped up in acquiring the latest and greatest tools, absorbing broader cybersecurity requirements, implementing security for the sake of security and disconnecting from real business needs.

Balancing security requirements with business needs has long challenged IT organizations, large and small.



(source)

Partnering with an MSSP is one way businesses reduce the requirements associated with maintaining cybersecurity programs, allowing executives to change their focus from the fear of a breach back to core business needs and their commitments to stakeholders, customers and employees.

4

SECURITY EXPERTISE

One critical lesson business leaders have learned over the past couple years is information security is more than technology. It is people, processes and technology – but the business side often seems to lose sight of the process piece. When implementing a security program, businesses need to align the program to their business needs, understand the risk tolerance of their business, put CIS, ISO or NIST controls in place, and set goals concerning how their organization should manage the controls and how to improve security posture without overspending.

Many organizations also face industry-specific challenges. Retail businesses often need to meet the Payment Card Industry Data Security Standard (PCI DSS), a complex set of security controls that includes access management, endpoint protection and secure development. Healthcare providers must meet the HIPAA Privacy Rule and Security Rule. Publicly traded companies must meet Sarbanes-Oxley (SOX) requirements. These are only a few of the industry-specific compliance challenges.



Quality MSSPs not only help businesses comply with regulations, but also help tailor their cybersecurity programs to the unique needs and risks of their specific industries. The right MSSP partner has experts to implement controls, manage risk and align IT security strategies to meet business goals. By tailoring cybersecurity services to the top risks and compliance needs of each business, MSSPs maximize return on investment while addressing the most pressing risks and needs.



ADVANCED TECHNOLOGY

A critical advantage of an MSSP is rooted in the technology it leverages to protect its clients. While the technology that fills the halls of RSA and Black Hat is leading edge, none of it provides a silver bullet. Even the best-of-breed layered security solutions have been compromised.

MSSPs have operated and tested most of this technology, and they've also built solutions organically based on what they have tested or integrated into their overall solutions. The benefit to the organizations they serve is that MSSPs use technology that matches the needs of their clients and the skillset of their clients' workforce.

MSSPs offer the best cybersecurity technologies to help businesses mitigate cybersecurity risk, they do so around the globe, for businesses of all sizes, in many different industries. This experience gives MSSPs the advantage of building defense solutions that can be adapted to a variety of customers and environments. This means there is a partner offering a solution tailor-made for each business need.

BY THE NUMBERS: THE MSSP SAVINGS PICTURE

EMPLOYEE COST SAVINGS

\$229,511 per company

Increased productivity; lower recruiting costs, salaries, up-front fees, faster deployment times, improved time-to-value on security investments



ROI

- Average investment: ***\$275,000 per 100 users***
- Average time to ROI: ***6 months***
- Average overall 3-year ROI: ***224%***
- Overall yearly savings: ***\$400,000 per 100 users***

According to [IDC research](#)



TECHNOLOGY COST SAVINGS

\$146,801 per year per 100 employees

provisioning, purchasing, managing equipment



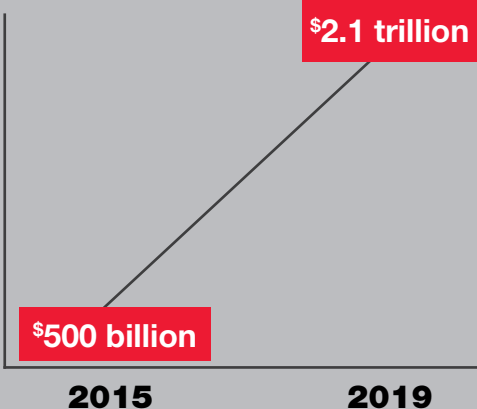
MANAGED SECURITY: SUPERIOR PROTECTION WITH LOWER COSTS

As cybersecurity risks and challenges continue to grow in complexity and impact, the cost of investing in full-scope layered cybersecurity programs has become prohibitively expensive. MSSPs provide the most advanced solutions, tailored to each business and industry-specific challenge, without large upfront capital expenses.

Superior protection, cost savings, business focus, security experts and leading-edge technology are some of the reasons why more executives choose managed security services to empower their security teams and enable their IT organizations to focus on strategic business needs.

NO SLOWING DOWN: SECURITY THREATS CONTINUE TO RISE

Cost of cybercrime for businesses



(source)

CALL 1.866.430.8166 FOR INFORMATION ON SECURITY SOLUTIONS, OR VISIT [HITACHI-SYSTEMS-SECURITY.COM](https://www.hitachi-systems-security.com) TO GET A QUOTE.

Hitachi Systems Security Inc.

955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada

Tel: +1 450-430-8166 Fax: +1 450-430-1858

www.hitachi-systems-security.com

FOR MORE INFORMATION

Learn more about how services from Hitachi Systems Security can help you secure your IT environment with minimum risk, realize the benefits of new technology or accelerate your journey to the cloud.

Visit www.hitachi-systems-security.com. 