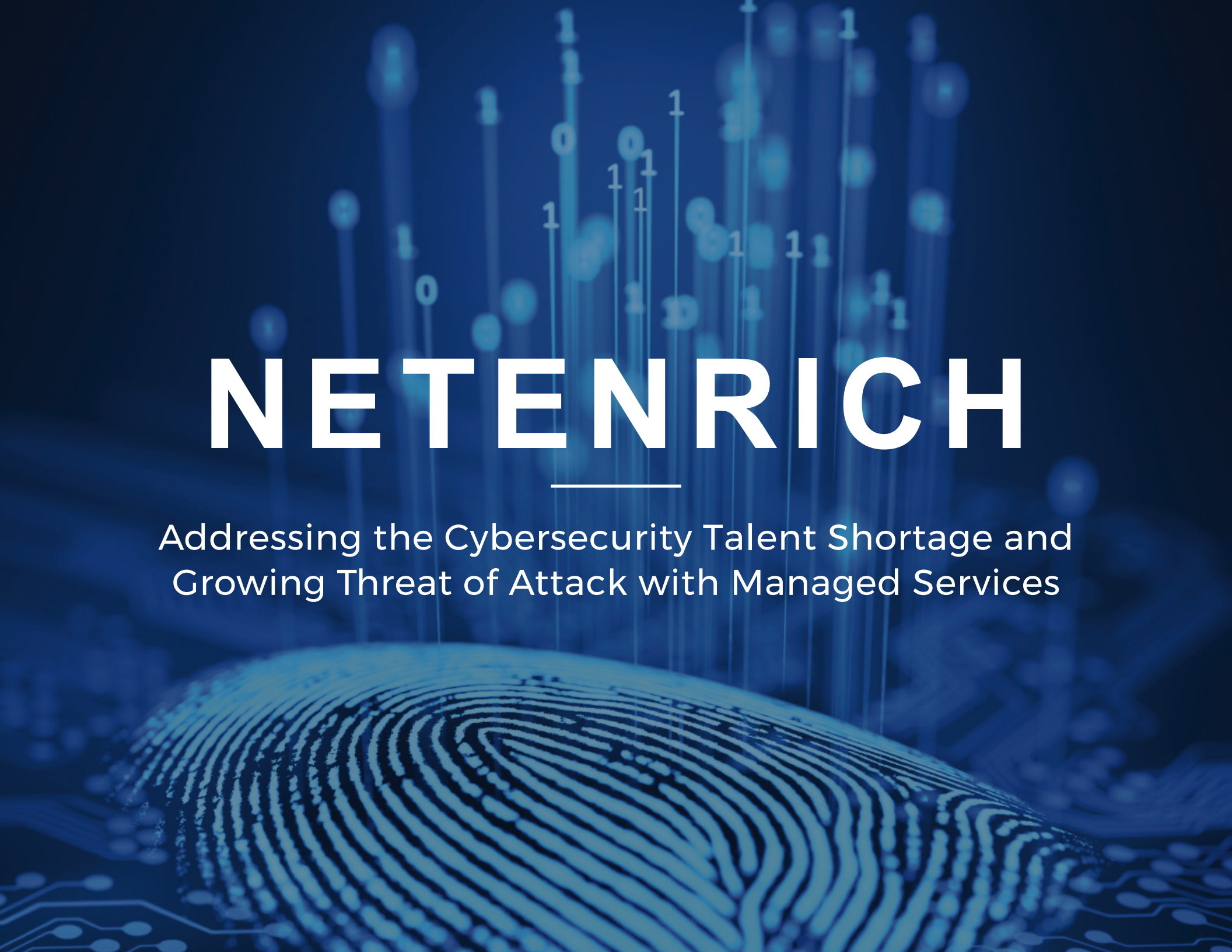

NETENRICH
Addressing the Cybersecurity Talent Shortage and Growing Threat of Attack with Managed Services

Addressing the Cybersecurity Talent Shortage and Growing Threat of Attack with Managed Services

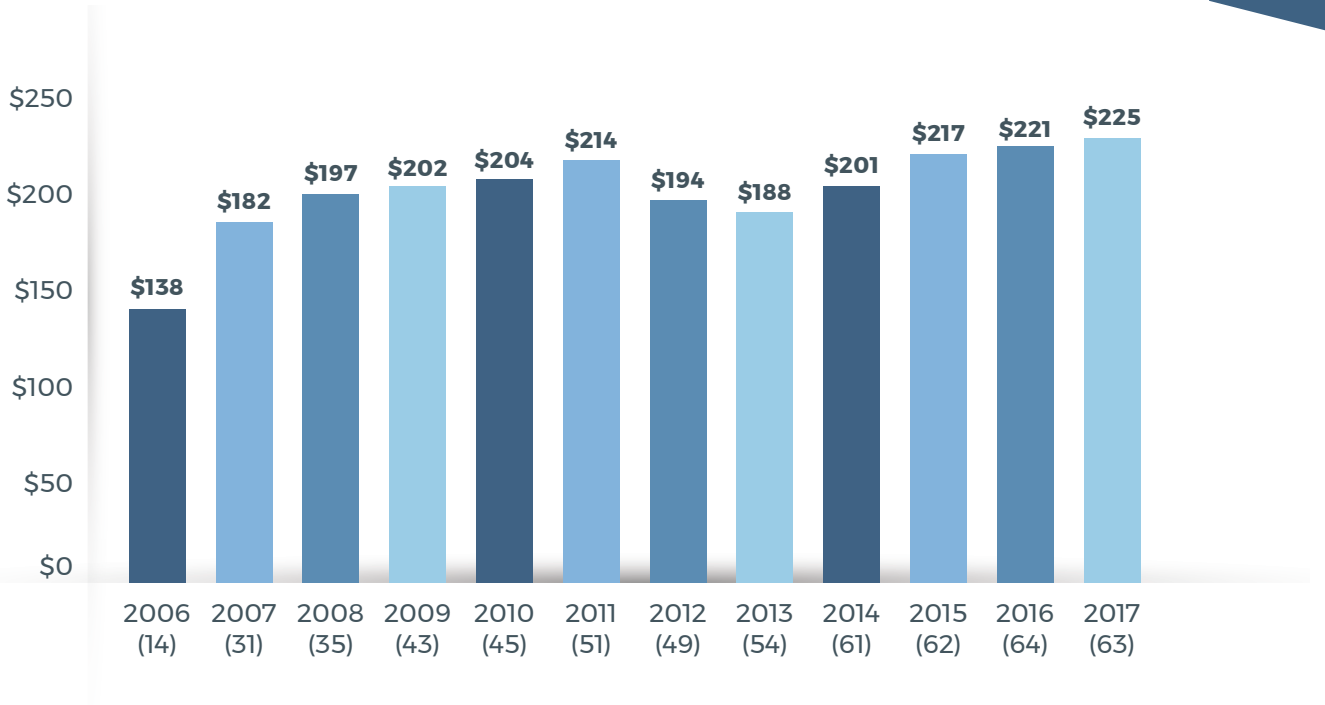
Cybersecurity is big business. Attacking unsuspecting businesses is now a $445 billion per year industry, with the average company facing as many as 200,000 security events per day.[1] With that kind of payoff on the line, more and new attacks seem inevitable.

The number of major data breaches in recent years is jaw-dropping and only growing bigger, with attacks becoming increasingly more sophisticated and malicious. Now, attacks targeting everyone from large enterprise organizations and government entities to smaller and mid-size businesses are putting everyone on edge and looking for some help.

1 "Cybersecurity has a Serious Talent Shortage. Here's how to Fix it." HBR.org. May 4, 2017.

The Average per Capita Cost of Data Breach Over the Past 12 Years

(Bracketed number defines the benchmark sample size)



In response, IT leaders are scrambling for solutions to protect their businesses, customers, and their bottom lines, but are also finding it much more challenging than anticipated because the number of qualified and affordable security professionals continues to dwindle.

The dearth of readily available talent has some leaders searching for alternative approaches, with many turning to Managed Services Solutions Providers (MSSP) to find the skills and headcount they need to stand up to today's security threats.

Source: https://www.bluefin.com/bluefin-news/closer-look-findings-ibm-security-ponemon-institutes-2017-cost-data-breach-study/

Increased threats, limited options for handling them

No business is immune to the threat of attack. In today's information ecosystem,with exponentially more data to manage and more points of entry, overall security can feel like an impossible task. Threats come from all angles; insider threats, malware and ransomware, along with DDoS and system or machine hacks all threaten the health and vitality of businesses across the spectrum.

Today's cyber threats are not only more numerous, but also more complex and destructive. According to a study from IBM Security and the Ponemon Institute, the average size of data breaches has increased 1.8 percent in the last few years to affect more than 24,000 records each. Not only are the attacks more substantive, they're more expensive too, as the average detection and escalation costs for activities such as forensic investigations, assessments and audit services increased dramatically from $730,000 in 2016 to $1.07 million in 2017, while data breach notification costs rose from $590,000 (2016) to $690,000 in 2017.

But the bad news doesn't end there.

Not only are companies spending more time and resources to identify and mitigate risk, they're also sacrificing revenue. Recent research by Cisco showed that nearly 30% of breached organizations—regardless of size or industry—experienced significant revenue losses on top of increased security expenses, amplifying the attacks' damage to the business[3].

3 "Cisco 2017 Annual Cybersecurity Report." Cisco.com

The Cost of Data Breaches[4]

$3.62M
per incident average cost of data breaches

1 out of 4
North American businesses will be affected each year

More than
24K
records accessed per breach

U.S. businesses have highest per breach losses,
$4.3M

As the negative business impacts from cyber threats continue to mount, organizations embracing preemptive measures such proactive monitoring and endpoint vulnerability assessments to minimize the damage will be best positioned to ward off future intrusions. ***But how?***

4 "2017 Cost of Data Breach Study: Global Overview." Ponemon Institute. 2017. https://www.ibm.com/security/infographics/data-breach/

Talent is expensive

While simply adding full-time staff seems like a logical solution, it's often more complex than it sounds. Most organizational leaders fear they are already ill-equipped to address security threats with existing resources and seek to bring on additional help to bolster their efforts. However, IT hiring managers are having a difficult time finding enough of the right talent to fully staff their security teams, and the shortage is only growing.

In fact, some sources show that there are currently more than one million unfilled cybersecurity positions around the globe and that many of the vacant roles are often never filled. That figure is expected to jump to approximately 1.8 million unfulfilled security positions by 2022[5], creating more competition for fewer resources.

The central issue facing IT security leaders is that the skills needed to successfully implement effective security programs are highly specialized, meaning that fewer professionals have them and those who do are difficult to find and expensive to hire—exponentially so for businesses in a rural or other outlying areas that aren't as attractive for on-site employees.

5 "Confront the Cybersecurity Talent Shortage." Gartner.com. June 23, 2017.

To add insult to injury, the cybersecurity career path is hardly recognized by young workers heading out into the workforce. Several studies indicate that career counselors or secondary education teachers rarely, if ever, suggest this path of study, fueling the ever-growing cyber talent gap.

Many companies seek to solve the lack of talent by cross-training their existing IT employees. While this may act as a band aid for the time being, it also assumes that current employees will want to make such a switch and start from scratch. The learning curve will most likely be steep and the outcome and time it takes to become proficient in key job functions is uncertain.

Other organizations may opt to hire and train the handful of cybersecurity specialists they find, but that solution doesn't come cheap either. More than half of industry decision makers agreed that a competitive salary is necessary to attract the strongest candidates and 60% believed good salaries contribute to better retention.[6] Naturally, increased competition for talent drives starting salaries higher, often pricing out businesses with fewer financial resources at their disposal. And as security roles continue to evolve--IDC predicts that 75 percent of chief security officers (CSO) and chief information security officers (CISO) will report directly to the CEO, not the CIO by 2018—salaries are likely to be pushed even higher.[7]

6 "The Most Critical Skills Gap: Cybersecurity." Fastcompany.com. July 27, 2016.
7 "Market Expansion Adds to Cybersecurity Talent Shortage." CSOonline.com. July 13, 2016

MSSPs: Expertise Meets Affordability

Managed Services Solution Providers bring a great deal to the table when it comes to solving these cybersecurity challenges, providing experienced talent, industry insight, and cost-effective solutions to meet most budgets.

Using a reputable MSSP to augment or supplement internal teams is a pragmatic and strategic approach, as MSSPs employ highly qualified and skilled staff capable of filling the gaps for managing and protecting customers' infrastructure and data. Businesses of all kinds are beginning to understand and embrace outside help, as the MSSP market's growth is outpacing security software growth by nearly a 2-to-1 margin[8].

An MSSP proactively addresses the issues and complexities that many large and mid-enterprise organizations face in an ever-changing environment. They come armed with diverse and interdisciplinary talent capable of securing every potential vulnerable area, while maintaining the flexibility and agility scale to their clients' specific needs.

More importantly, MSSPs possess the most up-to-date skills, qualifications and solutions to remain ahead of industry trends, whether it is perimeter and application security, vulnerability scanning, threat detection or compliance monitoring. In addition, many are proficient in driving operational excellence and boast decades of experience in IP and best practices.

8 "Roundup of Cloud Computing Forecasts, 2017." Forbes.com. April 29, 2017.

Predictable IT Costs

Given the option, business leaders will almost always choose cost certainty over unpredictability. When it comes to protecting mission-critical data and infrastructure, unpredictable costs shouldn't be the determining factor between sufficient protection and business disaster. Managed services convert variable IT costs tied to the break-fix or reactive mode of support into the stable costs of proactive support.

> ***What is simply a nuisance for well-staffed companies can be a debilitating hit for those with fewer resources or less expertise, and managed services can give IT leaders in both camps the certainty they need to more accurately project their business needs and allocate resources appropriately.***

Diverse skills and real-world experience

In-house IT employees often focus on a narrow set of potential problems, as their experience can be a limiting factor in how a company controls or prepares for a cybersecurity attack. Building an in-house Security Operations Center (SOC) can be costly and time-consuming because it requires a great deal of effort to maintain the talent and keep up-to-date with the latest security and compliance guidelines.

By contrast, MSSPs recruit from wider candidate pools, selecting the best, most credentialed talent from across IT disciplines and deploying those resources on-demand when a client demands. MSSPs employ diverse teams of professionals who've developed expertise across a number of functions through years of experience and then appoint an expert to serve as the lead for each function. As part of their role, the leads and their teams are required to maintain current certifications and are encouraged to pursue advanced credentials to stay ahead of trends. Together, MSSP teams encounter few problems they haven't come across already and can draw on the experience of other team members to overcome especially complex challenges in ways internal teams usually can't.

Competitive Edge

An MSSP model is a smart way of staying competitive when individual security talent is out of reach because of time, vulnerability profile, or budget concerns. MSSPs possess a deep understanding of security and governance issues, providing a foundation from which they can help clients better understand current security policies and advise on the steps needed to protect them from advanced and targeted threats.

Partnering with an MSSP gives organizations an agile and adaptable solution to address those issue, providing both the manpower and expertise to reassure prospective and existing customers that they're actively involved in security best practices with experts and create a distinct competitive advantage.

Benefits of working with MSSPs

Predictable Monthly Costs

Adaptable and Scalable Services On-Demand

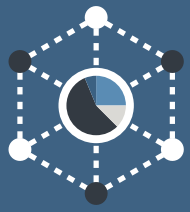
Expansive Knowledge Base and Expertise

Current Certifications and Credentials

NetEnrich Security Solutions: Resources, Reputation, & Reliability

As a leading MSSP, businesses of all sizes in an array of industries turn to NetEnrich's comprehensive security and IT infrastructure management services to tackle their biggest security challenges. More than 60% of cyber attacks effectively compromise their target organization and cause harm to its infrastructure, reputation and profitability in just minutes[9]. NetEnrich's CyberSecurity Services cast a wide net of protection, backing up existing security measures and filling in the gaps for total protection and peace of mind.

9 "28 Data Breach Statistics that will Inspire You to Protect Yourself." Bitsighttech.com. June 14, 2016.



Cyber Attack Readiness and Vulnerability

NetEnrich's Cyber Attack Readiness & Vulnerability Assessment Service is an essential solution for managing and thwarting threats and attacks on the digital perimeter and applications. Now, companies can better identify gaps or vulnerabilities in their current security posture and follow remediation guidelines to shore up defenses.

Monitoring Services for Security Devices

Security best practices suggest that organizations monitor of devices and IT systems around the clock, but many companies lack the necessary resources to do so. NetEnrich's Monitoring Services for Cloud proactively scans the entire network 24 hours a day, 7 days a week, 365 days a year for maximum protection. NetEnrich solutions include:

+ Security Monitoring
+ Incident Reporting
+ Antivirus
+ Malware Detection

on all security devices

Full compliance with corporate policies and regulatory standards such as PCI-DSS and HIPAA

A ***"single pane of glass"*** view of network devices and endpoints

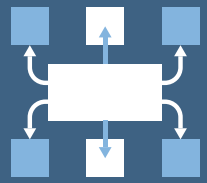
Management Services for Security Devices

Properly managing security devices requires specialized skills and round-the-clock vigilance. NetEnrich Management Services for Security Devices offloads the burden of continuous device monitoring, enabling internal teams to allocate resources to higher-priority tasks without sacrificing the safety or security of the devices. Specifically, NetEnrich's Management Services include:

Comprehensive management of
+ Firewalls
+ IDS & IPS
+ Secure Web Gateways
+ Web Application Firewalls (WAFs)

Managed identity and access for business processes and users

Integration of 3rd party SIEM (security and event management) tools and design approaches for log management



Threat Management Services

Threats are becoming more frequent, more advanced, and more complex. Blocking threats as they occur is key to staving off security breaches now and in the future. NetEnrich Threat Management Services protect infrastructure against advanced and targeted threats that attack business, customer data, payment details, and other sensitive information.

Handing off threat monitoring responsibilities allows customers to dramatically reduce the complexity and costs of their security systems and practices, while enhancing the protection of their most vital assets.

A Framework for a Secure Future

One out of six businesses will suffer a data breach in the next 24 months and seventy percent of those businesses will close their doors within a year of that breach.[10] It only takes a single visit to a malicious site from an employee to open the floodgates. Companies must find ways to bolster protection of their essential systems and data to survive.

Historically, organizations have relied on a hodgepodge of security devices and/or vendors to protect themselves from security threats. Such "solutions" take considerable time to manage and monitor and most organizations suffer from a severe lack of resources to meet the constraints, resulting in undue stress on IT personnel who are tasked with the extra responsibility. And for those companies that endeavor to hire cybersecurity professionals, they find slim pickings – a workforce short on talent and high on price.

CIOs and CISOs need to transform their security operations in data center, network, cloud, and end-use computing. Instead of wasting money on more tools and coming up short on a coherent security strategy, resources are better spent partnering with a managed security services provider to transform data center, network, cloud and end-use computing operations for maximum efficiency and security.

Companies should focus on what they do best. Security is truly everyone's problem; but that doesn't mean they should go it alone.

10 "2017 Cost of Data Breach Study." IBM.com. June, 2017.

NETENRICH

Visit NETENRICH.COM for more information about how our Managed Security Services can help cover gaps in your security operations and protect your organization from business-killing breaches.

NETENRICH.COM
1.408.436.5900