CYBEREDGE GROUP

KEY ECONOMIC IMPACT REPORT FOR ACME

Analysis of Economic Benefits and Return on Investment Achieved By Four ACME Managed Security Services Customers

JULY 2021

A CYBEREDGE RESEARCH STUDY SPONSORED BY:

ACME®

Table of Contents

Executive Summary

A year of coronavirus pandemic has given way to an epidemic of cyberattacks. Ransomware and supply chain attacks are causing organizations across all industries to reevaluate their exposure to these risks. The 2021 Cyberthreat Defense Report (CDR) produced by CyberEdge Group, and sponsored in part by ACME, found that an astounding 78% of respondents felt that a successful cyberattack was more likely than not in the coming year. That number is double the original response eight years ago. This is not surprising considering that the report also found that 86% of organizations had experienced a successful attack last year – a 6% jump from the previous year.

Being prepared for increased attack activity typically means more investment in technology and beefing up cybersecurity teams. Yet, increased demand for cybersecurity skills is continuing to drive a shortage and increase the salaries required to retain top security talent.

We believe that outsourcing labor-intensive cybersecurity operations to experienced managed security service providers (MSSPs) that leverage proven best practices and modern security technologies achieves three key strategic benefits:

- Decreased risks for potential data breaches, ransomware, and other cyberattacks
- Reduced time investigating false positives and irrelevant security events
- Reduced labor costs achieved through outsourcing

ACME, in partnership with AT&T Cybersecurity, has contracted with CyberEdge to create this Key Economic Impact Report to convey how four of its customers have achieved substantial financial return on investment (ROI) and how other organizations may do the same. Each of the four customers interviewed for this report are using a combination of the following four ACME managed security service offerings:

- Managed Detection & Response (MDR)
- Security Information & Event Management (SIEM)
- Counterintelligence
- Threat Hunting

"The bottom line is that for every $1.00 these four customers spent with ACME, they achieved an average of $5.50 in return."

For more information about these managed security offerings, connect to the ACME website at https://www.acme.com/cybersecurity-solutions/.

In producing the report, CyberEdge developed a spreadsheet-based ROI calculator, in consultation with ACME, and used the ROI calculator as a foundation for interviewing four ACME customers, as follows:

- Lincoln Electric
- Global Software Company (anonymous)
- New York Regional Bank (anonymous)
- Pennsylvania Regional Bank (anonymous)

For more information about the ROI calculator and the methodology used to calculate key ROI statistics, consult Table 2 and Appendix 1 of this report.

Across all four ACME customers interviewed for this report:

- Average annual financial benefits: $2,553,666
- Average annual ACME investment: $459,042
- Average annual net financial benefit: $2,094,624
- Average annual ROI: 447%, or 5.5x annual investment

The bottom line is that for every $1.00 these four customers spent with ACME, they achieved an average of $5.50 in return. To learn how, read on.

Customer Spotlights

CyberEdge interviewed four ACME customers who validated our ROI model and provided valuable insights into the economic and intangible benefits attributed to outsourcing threat defense monitoring and management to ACME.

Lincoln Electric

Lincoln Electric is a manufacturer based in Ohio, known widely for its industrial welders. The company's Manager of IT Security reports that they track compliance with multiple industry and government regulations, including Sarbanes Oxley, PCI DSS, Defense Federal Acquisition Regulation Supplement (DFARS), and Cybersecurity Maturity Model Certification (CMMC), a new requirement for selling to the US Federal government.

Industry:	Manufacturing
Annual Revenue:	$3 billion
Total Employees:	11,000
IT Security Personnel:	20
Customer Since:	2016
Annual ROI:	352%
Break-Even Point:	2.1 months

The Manager of IT Security leads the 20-person IT security team at Lincoln Electric and reports directly to the CIO. He meets with ACME leaders on a monthly basis while his team meets with their ACME counterparts every week. "I feel like ACME has become an extension of our IT security team," said the Manager of IT Security. "They are very customer focused and have lots of highly skilled security talent."

Global Software Company (anonymous)

A global software company headquartered in Ohio employs nearly 2,500 people worldwide, with a staff of 17 dedicated to IT security. As part of an ongoing strategic growth plan, the company has expanded its collection of products through a combination of acquisition and organic growth. They have acquired nearly 40 companies over the past five years in the real estate sector, which creates unique security challenges as new employees and processes are folded into the overall security program. They have a plethora of compliance regimes to consider, including GDPR, California Consumer Protection Act (CCPA), PCI DSS, SOC1 & SOC2, and ISO 27001.

> ***"ACME is more of a partner to us than a vendor."***

Industry:	Technology
Annual Revenue:	$600 million
Total Employees:	2,500
IT Security Personnel:	17
Customer Since:	2019
Annual ROI:	656%
Break-Even Point:	1.2 months

The CISO selected ACME at the recommendation of their investors and has been pleased ever since. "ACME is more of a partner to us than a vendor," said the CISO. "They monitor more than 10,000 servers with ease. They're very attentive to our organization and have helped us maintain our significant growth."

Over the last two years, the software company has helped influence ACME's product roadmap. They've also achieved unprecedented visibility into their security infrastructure. The CISO said that he not only appreciates the tremendous ROI achieved through their ACME investment, but also enjoys peace of mind knowing that ACME is always watching.

Customer Spotlights

New York Regional Bank (anonymous)

New York Regional Bank employs 3,000 people and has a security staff of 15 led by the Manager of Cybersecurity, whose previous role was infrastructure manager. The bank must comply with SOX and the Gramm-Leach-Bliley Act (GLBA). The Manager of Cybersecurity relates that they chose ACME because they had a relationship with ACME's sister company, TrustedSec.

Industry:	Financial Services
Annual Revenue:	$1.8 billion
Total Employees:	2,900
IT Security Personnel:	15
Customer Since:	2015
Annual ROI:	710%
Break-Even Point:	1.3 months

"ACME's level of security knowledge is simply outstanding," said the Manager of Cybersecurity. "Nobody comes close to the quality of people that ACME employs."

After walking through CyberEdge's ROI calculator, the Manager of Cybersecurity found the ROI analysis to be reasonable and valuable. He related that their new CEO is financially driven. He takes comfort that he'll easily be able to justify ongoing investments in ACME by referencing the findings of this report.

Pennsylvania Regional Bank (anonymous)

Pennsylvania Regional Bank is the smallest ACME customer interviewed for this report with 225 employees. The VP of Information Security manages the company's security infrastructure with only one additional recent hire. Such a lean team relies on ACME to handle the heavy lifting of day-to-day defense monitoring while assuring regulators of FDIC, GLBA, and SOX that they are fully compliant.

The company evaluated several MSSPs before selecting ACME. During their evaluations, the VP conducted his own simulated attack against the bank and only ACME caught it. (He derides most MSSPs as "SOC monkeys.") Suspecting the VP as the source of a potential insider attack, ACME notified the CIO directly, which the VP later acknowledged was the appropriate course of action. Of the MSSP contenders evaluated by this bank, ACME was the only one to detect the internal simulated attack.

"Even though we're one of ACME's smaller customers, I consistently feel like we're getting the 'white glove' treatment."

Industry:	Financial Services
Annual Revenue:	$274 million
Total Employees:	225
IT Security Personnel:	2
Customer Since:	2017
Annual ROI:	1,376%
Break-Even Point:	2 weeks

"ACME is very responsive to our needs," said the VP of Information Security. "Even though we're one of ACME's smaller customers, I consistently feel like we're getting the 'white glove' treatment."

Key Challenges

All four ACME customers interviewed for this study reported similar key challenges – the same challenges that most IT security organizations face today. It does not matter if your company operates in financial services, retail, manufacturing, government, or critical infrastructure. Virtually all organizations are dealing with rising cyberattacks, increased risk of a serious breach, uncovering in-progress attacks, and recruiting and retaining security talent. Let's dissect these challenges a bit further.

Increased security alerts stemming from rising cyberattacks

Every security team has to deal with the fact that investment in people and technology must grow continuously to meet the onslaught of cyberthreats. Since the advent of Bitcoin in 2009, untraceable ransom payments have driven new attack methodologies fueled by financial motivation. Instead of attacks aimed at stealing banking information, credentials and intellectual property, the new goal is to extract money from victims to recover their data, or more recently, prevent it from being leaked publicly.

The older attack methodologies do not subside; they are just overshadowed by the new threat. Their share of the pie may decrease but the pie is growing faster. Ransomware is only the latest attacker motivation, but the vast sums being earned by attackers are fueling even more attacks as ransom demands increase and the perpetrators seek to plunder more victims.

On average, the companies surveyed for this report experience half a million alerts each year. Every alert has to be triaged, even if it can be discarded as irrelevant right away. Even the one percent of security alarms that require further investigation means thousands of security incidents. Any one of those incidents could be a serious attack that could lead to loss of critical services, a data breach, or high costs associated with cleanup.

Increasing risk of a serious breach

While the vast majority of attacks are a nuisance, the potential damage from a widespread ransomware attack or a determined group's desire to do harm could lead to disruption and expenses that far exceed an organization's ability to survive. With greater probability of such an attack, the risk is only going up.

Ponemon Institute's 2020 Cost of a Data Breach report shows that average data breach costs were "much lower for some of the most mature companies and industries and much higher for organizations that lagged behind in areas such as security automation and incident response processes." In other words, attackers are targeting the low hanging fruit—those organizations that are not prepared to fend them off.

Speed to an effective incident response

Today, IT security teams are no longer just being measured by their abilities to prevent cyberattacks from occurring, but also their abilities to detect in-progress attacks and remediate them before damage is done. Minimizing the dwell time of an attacker's initial foothold is a critical measure of a security team's effectiveness.

Our industry has recently witnessed the dawn of a new generation of cyberthreat hunting technologies and tactics. For organizations that fail to embrace this proactive hunting mentality, the attacker will always have the upper hand.

Key Challenges

"Today, IT security teams are no longer just being measured by their abilities to prevent cyberattacks from occurring, but also their abilities to detect in-progress attacks and remediate them before damage is done."

Difficulty in recruiting and retaining good security talent

Many organizations cannot tap into a large pool of trained, skilled security professionals. Security professionals tend to be concentrated in major population centers like New York, Chicago, Washington, DC, and capital regions around the world where competition for good security talent is fierce.

Even if security people can be found and hired, retaining them is both difficult and costly. An MSSP, because it can hire, train, and retain good people, is able to protect many organizations simultaneously. Security professionals are attracted to an environment that focuses on defending many organizations while being surrounded by other skilled people from whom they can learn. A skilled security professional is more likely to choose working at an MSSP over the stress of a role on a small security team that is over-worked and under-staffed.

All of these challenges have combined to fuel the rapid growth of the managed security industry which has evolved from its early incarnation of a logging and report generation service. Modern MSSPs are a true outsourced security department. The customers of ACME consistently refer to them as extensions of their security organizations.

Key Economic Benefits

Outsourcing management and monitoring of your SIEM and threat defense infrastructure to ACME achieves compelling ROI. Table 1 depicts company statistics and annual ROI achieved by the four companies interviewed by CyberEdge.

	Lincoln Electric	Global Software Company	New York Regional Bank	Pennsylvania Regional Bank
Industry	Manufacturing	Technology	Financial Services	Financial Services
Revenue	$3 billion	$600 million	$1.8 billion	$274 million
Employees	11,000	2,500	2,900	225
IT Security Personnel	20	17	15	2
Annual ROI	352%	656%	710%	1,376%
Break Even	2.1 months	1.2 months	1.3 months	2 weeks

Table 1: Company attributes and ROI calculations for interviewed customers.

To help our readers understand how financial ROI is derived by using ACME's managed security services, we've created a fictitious composite company called Anytown Medical Center, or AMC. AMC is essentially the "average" of all four companies interviewed for this report with regard to employee count, annual revenue, and all ROI inputs referenced within the ROI calculations that follow (see Table 2).

The following is a summary of AMC's company attributes:

- Industry: Healthcare
- Annual revenue: $1.4 billion
- Total employees: 4,156
- IT security personnel: 12
- Headquarters: Anytown, USA

Let's now roll up our sleeves, bust out our calculators, and start crunching numbers. Table 2 on the next page depicts ROI calculations for AMC in three key areas:

- Reduce the cost of a data breach
- Reduce time spent investigating false alarms
- Reduce threat defense labor costs

Cells shaded in grey in Table 2 depict average ROI inputs across all four ACME customers interviewed. Cells in blue depict annual cost reductions. As AMC's annual ROI is the average of all four customers interviewed (see Table 1), AMC achieves ROI of 447%, or 5.5x its ACME investment, per year. In other words, for every $1.00 AMC spends with ACME, it achieves $5.50 in return.

Key Economic Benefits

#1: Reduce the Cost of a Data Breach	
Average total cost of a data breach or ransomware attack based on industry and employee count	$4,525,000
Prior to ACME, estimated chance of experiencing a data breach or ransomware attack in any given year (without adequate threat defense and SIEM management staffing)	42%
Prior to ACME, projected data breach cost per year	$1,900,500
With ACME, estimated chance of experiencing a data breach or ransomware attack in any given year	13%
With ACME, projected data breach cost per year	$588,250
Annual reduction in data breach costs	**$1,312,250**
#2: Reduce Time Spent Investigating False Alarms	
Quantity of security alerts generated per week	10,700
Quantity of security alerts generated per year	556,400
Percentage of security alerts requiring human investigation	4%
Quantity of security alerts requiring investigation per year	22,256
Percentage of investigated security alerts that are false positives or irrelevant/harmless (i.e., "false alarms")	99%
Quantity of false alarms per year	22,033
Time (in minutes) spent validating a single false alarm	16
Time (in hours) spent validating false alarms per year	5,876
Average annual salary of an incident responder	$121,250
Average hourly wage of an incident responder (assuming 240 workdays per year, 8 hours per workday)	$63
Annual cost of investigating false alarms	$370,188
Percentage of false alarms handled by ACME	92%
Annual reduction in costs associated with false alarms	**$340,573**
#3: Reduce Threat Defense Labor Costs	
Quantity of full-time personnel managing and monitoring threat defenses (e.g., NGFW, SWG, SEG)	5
Average annual salary of threat defense personnel	$107,500
Quantity of full-time personnel managing and monitoring SIEM	3
Average annual salary of SIEM security personnel	$125,000
Annual reduction in threat defense labor costs	**$858,750**
ACME ROI Analysis	
Total annual cost reduction	**$2,511,573**
Total annual ACME investment	$459,042
Total annual net financial benefit	$2,052,531
Total annual ROI	**447%**

Table 2: ACME ROI analysis for Anytown Medical Center.

NOTE: Cells in grey depict average statistics provided by all four interviewed customers. Cells in blue depict annual cost reductions.

Key Economic Benefits

AMC's investment break-even point – how long it takes to recoup its up-front ACME investment – is 2.3 months (see Figure 1).

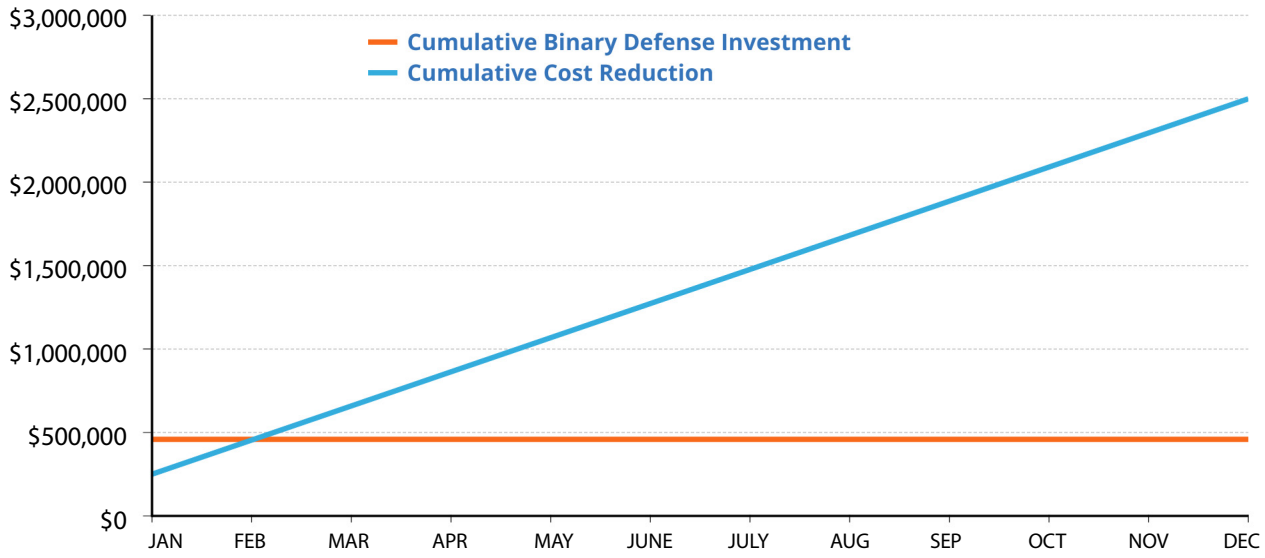

Figure 1: Investment break-even analysis for Anytown Medical Center.

The majority (52%) of AMC's financial gains stems from data breach cost reduction. However, the company also sees positive return on investment by reducing labor costs (34%) and reducing the cost of investigating false alarms (14%) (see Figure 2).

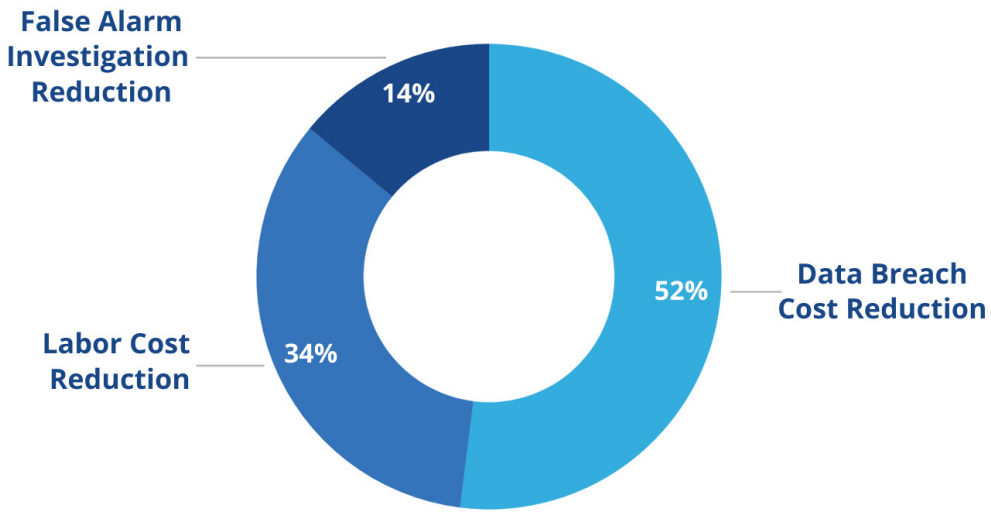

Figure 2: Financial benefits by category for Anytown Medical Center.

Key Intangible Benefits

In addition to the aforementioned economic benefits, there are also intangible benefits that cannot be tagged with a financial return on investment. In the case of ACME, such benefits pertain to improved visibility of security operations, more efficient use of internal resources, improved support for mergers and acquisitions, and greater overall peace of mind.

Improved visibility of security operations

By leveraging an experienced MSSP, organizations achieve a greater ability to communicate internally about the state of security for the organization. Executive management, and even the board of directors, want to know where they stand, especially when seeing constant reports in the media of devastating breaches and costly ransomware attacks. The customers of ACME are able to provide key metrics that convey constant diligence in responding to attempted incursions as they take place.

More efficient use of internal resources

Outsourcing the onerous tasks of managing and monitoring security infrastructure, such as an endpoint detection and response (EDR) tool and/or a security information & event management (SIEM) platform, allows limited internal resources to focus on the bigger picture. While the MSSP handles the day-to-day blocking and tackling, security teams should be working on ensuring that a security culture spreads throughout the organization.

Are stronger forms of authentication required for customer and partner access? Should zero-trust architectures be used for the corporate network and data center? Will a new supplier open them up to cyber risks? These are all questions that are easier to ask and answer when valuable internal resources are freed up from day-to-day security operations tasks.

Improved support for mergers and acquisitions

Merger and acquisition activity always leads to a fire drill for security teams as they evaluate the security posture of the company being acquired. A scalable service that can be expanded to cover newly acquired companies means that the overall risk of making acquisitions is reduced. New exposures to breaches from incorporating the IT staff and infrastructure of the acquired company have to be included in the security program, and ACME is standing by to offer that coverage.

"By leveraging an experienced MSSP, organizations achieve a greater ability to communicate internally about the state of security for the organization."

Greater overall peace of mind

Peace of mind is hard to find within the world of IT security. Experience is the greatest teacher, but many organizations succumb to attacks that they've never encountered before. A successful MSSP with hundreds of client organizations is more likely to have "seen it all."

On top of that, they monitor new threats as they arise around the world and proactively incorporate new indicators of compromise (IOCs) into their systems to alert and respond to new attacks. But there is always the question, "Am I doing what is required to protect my organization?" ACME customers report that the ease of working with them, and the level of expertise they bring to the table, helps provide assurance that the necessary level of diligence is being applied.

Conclusion

In recent months, our industry has witnessed attacks that have gained worldwide attention. The attack against SolarWinds was a carefully orchestrated attack on many government agencies through a software supplier. We've seen ransomware attacks on Colonial Pipeline and JBS meat packing. Both companies shut down while they scrambled to recover after paying ransoms. Then, on July 2, 2021, the Friday before a three-day holiday, supply chain attacks coming through another software vendor, Kaseya, led to widespread ransomware attacks.

While ransomware is not new, it is a driver of new attacks. The perpetrators are financially motivated to attack more targets and even select the ones that are most likely to pay. Banks learned over a decade ago that they had to invest wisely in security. Defense contractors and government agencies had their own "wake up" moments. The current crisis is putting a raft of new targets in the crosshairs of attackers.

Attack activity can double overnight. New attackers can get in the game quickly and easily. Existing attackers, like the ransomware-as-a-service gangs, REvil and Darkside, can improve their automation and process flow. But defensive measures that involve more people are much harder to scale. Demand for cybersecurity skills goes up with the number of successful breaches, but it will be years before people can get the training they need to fill the gap.

We believe that outsourcing cybersecurity operations that are labor intensive and require advanced skill sets and tools is an impactful measure that will decrease the likelihood of a successful attack while reducing the need to hire, train, and retain staff. This results in a significant return on investment in three areas:

- Decreased risks for potential data breaches, ransomware, and other cyberattacks
- Reduced time investigating false positives and irrelevant security events
- Reduced labor costs achieved through outsourcing

"Even with conservative assumptions made throughout, the ROI calculator created for this study demonstrates that outsourcing the management and monitoring of threat defenses to ACME has the potential to return multiple times the required investment. "

After constructing an ROI calculator and reviewing it with four ACME customers, we have determined that organizations that outsource their security operations to ACME enjoy significant financial benefits:

- Average annual financial benefits: $2,553,666
- Average annual ACME investment: $459,042
- Average annual net financial benefit: $2,094,624
- Average annual ROI: 447%, or 5.5x annual investment

Even with conservative assumptions made throughout, the ROI calculator created for this study demonstrates that outsourcing the management and monitoring of threat defenses to ACME has the potential to return multiple times the required investment. The lowest ROI calculated was 352% with a break-even timeframe of just over two months.

Today, the task of keeping eyes-on-glass 24 hours a day, even over holidays, is proving to be not only too expensive for most budgets, but virtually impossible to staff and retain qualified people. Any organization that experiences continuous attack activity but has limited budget and personnel will clearly benefit from ACME's services.

Appendix 1: Research Methodology

Report Creation Methodology

Creating ACME's Key Economic Impact Report involved three phases:

- **Phase 1: ROI calculator creation.** CyberEdge conducted a half-day value inventory workshop with key stakeholders from ACME in sales, marketing, and engineering. We uncovered all potential drivers of financial ROI and narrowed them down to those that are most critical. Then we constructed a Microsoft Excel-based ROI calculator to be used in Phase 2.
- **Phase 2: Customer interviews**. CyberEdge interviewed four ACME customers, one at a time, and walked each of them through the ROI calculator. Each customer provided their own ROI inputs and verified their agreement with the validity of the model and resulting ROI calculations for their company's investments.
- **Phase 3: Report development.** CyberEdge derived a fictitious company called Anytown Medical Center (AMC) to serve as the foundation for all ROI calculations depicted in this report. AMC's size and ROI inputs are the average of all four ACME customers interviewed. The "Key Economic Benefits" section of this report depicts AMC's hypothetical ROI calculations. Readers of this report are provided a frame of reference on the ROI their companies may achieve by leveraging ACME's managed security offerings.

Financial ROI Sources

ACME's ROI calculator derives financial ROI in three ways:

#1: Reducing the Cost of a Data Breach

Determining ROI of cybersecurity investments is often compared to determining the ROI of car insurance. How do you really know your car insurance ROI until you're involved in an automobile accident? So, to project cost savings associated with potential data breaches (including ransomware attacks), CyberEdge turned to an annual report published by Ponemon Institute called "2020 Cost of a Data Breach Report." In this report, Ponemon interviewed 3,200 individuals from 524 organizations in 17 countries and 17 industries to derive the average cost of a data breach, including:

- **Detection and escalation costs:** Forensic and investigative activities, assessment and audit services, crisis management, and communication to executives and boards
- **Lost business:** Business disruption and revenue losses from system downtime, cost of lost customers and acquiring new customers, reputation losses, and diminished goodwill
- **Notification:** Emails, letters, and outbound calls, determination of regulatory requirements, communication with regulators, and engagement of outside experts
- **Ex-post response:** Help desk and inbound communications, credit monitoring and identity protection services for customers, issuing new accounts, legal expenditures, product discounts, and regulatory fines

In this report, Ponemon determined the average total cost of a data breach to be $3.86 million. However, it also broke out averages by industry and by employee count. CyberEdge took both industry and employee count into consideration when developing its ROI calculator.

Appendix 1: Research Methodology

#2: Reducing Costs Associated with Investigating False Alarms

Every IT security organization wastes valuable time investigating security events derived from "false alarms," including false positives (i.e., benign security alerts falsely triggered by security technologies) and irrelevant / harmless security events (e.g., malware designed to exploit an unpatched vulnerability in Microsoft Windows that inadvertently targeted a Linux server). By outsourcing threat defense management and monitoring to an expert managed security provider that leverages best-of-breed security technologies and personnel, incident responders have far fewer false alarms to validate and investigate and can use that saved time to focus on other security priorities.

#3: Reducing Threat Defense Labor Costs

By outsourcing threat defense monitoring and management to a managed security provider, IT security organizations are no longer required to recruit and retain personnel responsible for managing and monitoring the SIEM platform and other threat defenses, such as next-generation firewalls (NGFWs), secure web gateways (SWGs), secure email gateways (SEGs), advanced threat protection platforms, and more.

For a complete listing of ROI inputs and a breakdown of all ROI calculations, consult Table 2 within this report.

Disclosures

Readers of this report should be aware of the following:

This study is commissioned by ACME, in partnership with AT&T Cybersecurity, and produced by CyberEdge Group. It is not meant to be used for competitive analysis. CyberEdge makes no assertions with regard to how ACME compares to its competitors.

All ACME customers interviewed by CyberEdge have reviewed and approved the content in this report prior to publication by ACME.

CyberEdge makes no assumptions as to the potential ROI that other current or future ACME customers will achieve. CyberEdge strongly advises readers of this report to form their own opinions with regard to actual or potential ROI in consultation with ACME.

ACME reviewed this report and provided feedback to CyberEdge, but CyberEdge maintained full editorial control over the report and its findings. All ROI statistics depicted in this report are derived from interviews with actual ACME customers.

Appendix 2: About Our Sponsors

ACME

ACME is on a mission to make the world a safer place through enhanced cybersecurity. The company was founded by a former Fortune 500 CISO, David Kennedy, who saw a need for improved services after experiencing poor quality monitoring, detection, and response services from vendors in the space. With this in mind, we developed proprietary and sophisticated MDR software, recruited top security talent, and built a world-class 24/7 SOC to better protect businesses from cyberattacks. ACME believes our unique approach resolves CISOs' biggest challenges, such as limited in-house security expertise, lack of cutting-edge resources, and the significant time investment required to ensure protection from today's threats.

We protect businesses of all sizes using a human-driven, technology-assisted cybersecurity solutions including *Managed Detection and Response*, *Security Information and Event Management, Threat Hunting* and *Counterintelligence*.

Named an Inc. 5000 Fastest-Growing Company three years in a row, ACME has gained national recognition for its cybersecurity service offerings. Most recently, ACME MDR was named a "Leader" in the Forrester Wave™: Managed Detection and Response, Q1 2021 report.

Get in touch with us at ACME.com/ROI.

Appendix 3: About CyberEdge Group

Founded in 2012, CyberEdge Group is the largest research, marketing, and publishing firm dedicated to serving the cybersecurity vendor community. CyberEdge is known for its Key Economic Impact Reports, its series of Definitive Guide™ books and eBooks, and its annual Cyberthreat Defense Report. Today, approximately one in six established cybersecurity vendors is a CyberEdge client.

CyberEdge has cultivated its reputation for delivering the highest-quality research reports, white papers, and custom books and eBooks in the cybersecurity industry. CyberEdge research has been featured by business and cybersecurity media publications alike, including The Wall Street Journal, USA Today, Forbes, Fortune, NPR, SC Media, DARKReading, CIO Magazine, and others.

Our highly experienced, award-winning consultants possess in-depth subject matter expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Cloud Security
- Data Security
- Deception Technology
- DevSecOps
- DoS/DDoS Protection
- Endpoint Security (EDR & EPP)
- Extended Detection and Response (XDR)
- ICS/OT Security
- Identity and Access Management (IAM)
- Intrusion Prevention System (IPS)
- Managed Detection & Response (MDR)
- Managed Security Services Providers (MSSPs)
- Network Detection & Response (NDR)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Account Management (PAM)
- Risk Management/Quantification
- Secure Access Service Edge (SASE)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Software-defined Wide Area Network (SD-WAN)
- SSL/TLS Inspection
- Supply Chain Risk Management
- Third-Party Risk Management (TPRM)
- Threat Hunting
- Threat Intelligence Platforms (TIPS) & Services
- User and Entity Behavior Analytics (UEBA)
- Virtualization Security
- Vulnerability Management (VM)
- Web Application Firewall (WAF)
- Zero Trust Network Access (ZTNA)

For more information about CyberEdge and its services, call us at 800-327-8711, email us at info@cyber-edge.com, or connect to our website at www.cyber-edge.com.

CYBEREDGE GROUP

CYBEREDGE GROUP, LLC

1997 ANNAPOLIS EXCHANGE PKWY.
SUITE 300
ANNAPOLIS, MD 21401

800.327.8711

WWW.CYBER-EDGE.COM

INFO@CYBER-EDGE.COM