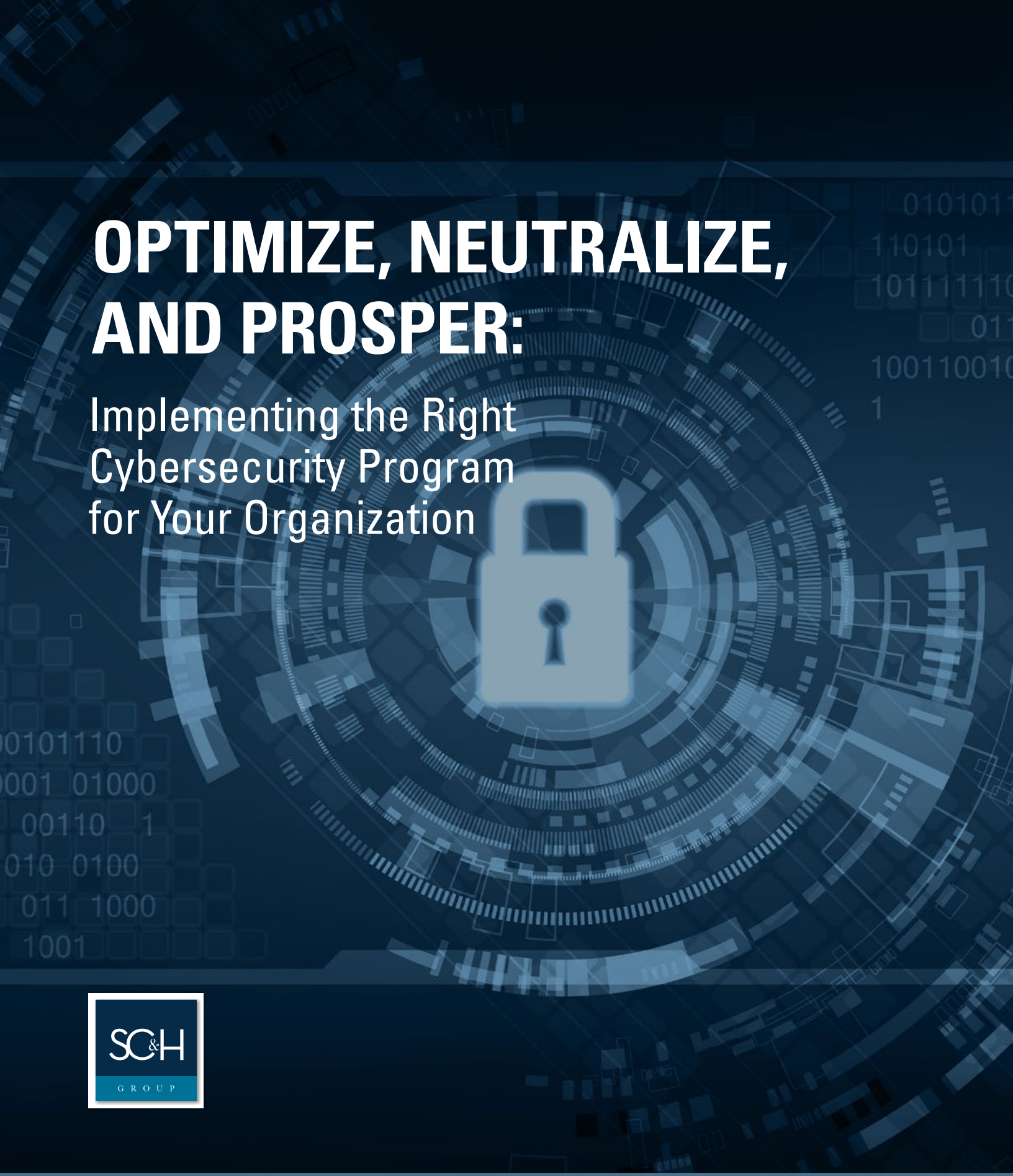
OPTIMIZE, NEUTRALIZE, AND PROSPER:

Implementing the Right Cybersecurity Program for Your Organization



SC&H GROUP

Introduction

In recent years, reports of massive data breaches have been commonplace, from Equifax's now legendary breach—which exposed the personal identity information (PII) of over 145 million consumers—to attacks on various Fortune 100 companies.

However, it's not just large companies that have been affected. While media attention has focused on high-profile breaches, cyber attacks have become routine across nearly every company size, type, location, and industry.

In fact, more than 61 percent of mid-sized organizations have experienced a cyber attack in the last 12 months, and 57 percent of all organizations have had a recent, significant cybersecurity incident. Overall, the number of organizations impacted by a cyber attack has increased by 11 percent in the last year.[1,2]

As breaches continue to grow in size and severity, is your organization doing everything possible to address cyber threats? Don't be so sure.

KEY CYBERSECURITY STATS: TODAY'S ORGANIZATIONS*

57%	Have experienced a recent, significant cybersecurity incident
54%	Have experienced a data breach involving PII in the last year
	HOWEVER...
88%	Do not consider information security in their strategy and planning
79%	Rate their ability to mitigate cyber attacks as less than "highly effective"
58%	Consider cybersecurity only a "moderate" or "minimal" concern

Though executives are mostly confident that their organization can predict, detect, and prevent a sophisticated cyber attack, only 22 percent fully consider information security in their organizational strategy and planning.[2]

Given the substantial operational, economic, and reputational liability that accompanies a cyber attack, it is critical that executives make cybersecurity an organizational priority by:

- Identifying the far-reaching risks and effects of data breaches
- Overcoming common barriers to ensuring effective cybersecurity measures
- Using this insight to develop a new or improved cybersecurity program that focuses on your operations, not just your technology

With awareness, commitment, and a comprehensive program that addresses your organization's biggest cybersecurity risks, you can set the foundation for more dependable performance and long-term success.

---

*Sources:

1 - 2017 Ponemon Institute / Keeper Security State of Cybersecurity Survey

2 - 2017 EY Global Information Security Survey

3 - 2017 Nexia International Global Cybersecurity Report

4 - 2017 Ponemon Institute / IBM Cost of Data Breach Study

CONTENTS

IDENTIFYING THE RISKS OF INADEQUATE CYBERSECURITY MEASURES

When examining the consequences of a potential cybersecurity incident, your first consideration is likely the exposure of critical data. Indeed, the effects of a security breach typically begin with data exposure, whether intellectual property, financial data, or customer/employee data, such as PII and protected health information (PHI).

But, the risks associated with a breach extend far beyond the initial data exposure—to virtually every aspect of your organization's value and performance. Key risks can be classified in several areas, including operational, financial, legal/regulatory, reputational, and strategic.

AREA OF RISK	POSSIBLE EFFECT ON YOUR ORGANIZATION
Operational	Delays, service interruptions, and ineffective processes
Financial	Loss of financial resources and new/recurring business
Legal/ Regulatory	Costly legal and regulatory penalties
Reputation	Short- and long-term damage to your organization's brand
Strategic	Weakened ability to achieve key objectives

Operational Risks

A cybersecurity incident can cause serious interruptions to service delivery and internal efficiency within business and IT activities.

For instance, in the aftermath of a cyber attack, the disruption to normal business operations has cost mid-sized businesses an average of $1.2 million per incident over a 12-month period. Further, they have spent an average of $1 million to address theft of or damage to their technology assets.[1]

Within IT operations, organizations must maintain sound processes to not only collect cybersecurity information, but also update all potentially affected systems.

Similarly, you must maintain sound processes within business activities, ensuring that sensitive financial, employee, customer, and company information is not shared without proper validation and authorization.

Financial Risks

The financial risks of a breach are one of the top concerns to many executives—and for good reason. Each risk area has a financial cost, whether short-term (e.g., service interruption) or long-term (e.g., damage to brand and reputation).

Cyber attacks cost the global economy over $450 billion in 2017, with an average annual cost of more than $9.5 million per mid-sized company to manage incidents and recover from disruptions to customers and the business.[4]

Drilling down further, each security breach cost U.S. organizations an average of $79 in direct costs and $146 in indirect costs—per compromised record.[4] Considering that the average breach exposes more than 9,300 records, the financial costs can quickly add up.

Direct costs relate to activities needed in the aftermath of a data breach discovery, such as legal fees, consulting fees, and identity protection services for victims. Meanwhile, indirect costs relate to activities such as resource allocation, loss of customers, and damage to the company reputation, as well as employee efforts to:

- Discover the breach and investigate its cause
- Identify and notify the people whose data has been compromised
- Conduct necessary communications and public relations campaigns

While executives are concerned about the financial risks of a cyber attack, many aren't fully aware of the extent of those risks. In fact, nearly half (49 percent) of companies that experience a data breach don't know what financial damage it has caused.[2]

Legal/Regulatory Risks

The aftermath of a data breach can put your organization at risk of substantial legal and compliance expenses—due in part to cybersecurity requirements enacted by industries and government agencies.

For instance, depending on your organization's industry, customers, location, ownership status, and other qualities, you may be required to maintain a wide range of cybersecurity procedures and practices. Requirements have been put in place by industry regulatory bodies and state legislatures, as well as various federal government agencies, including the Securities and Exchange Commission, Federal Trade Commission, and others.

Rather than try to determine if they qualify for an exemption to the many new and proposed data security regulations, organizations should focus on implementing an effective cybersecurity program.

Looking forward, regulations will continue to strengthen, and it is likely that consumers will eventually be able to sue organizations directly for data breaches.

So, rather than try to determine if your organization qualifies for an exemption to these or the many other existing and proposed regulations, it is advisable to instead focus on developing and implementing a comprehensive cybersecurity program.

Reputational and Strategic Risks

Each of the risk areas above converge to pose major reputational and strategic risks.

As existing and potential customers become aware of breaches via company communications and/or local and national media coverage, the strength of your organization's brand can be seriously damaged. While not as overt as the immediate financial and operational consequences of a breach, this damage can ultimately be more harmful to your business.

Consider the loss of customers from a breach. There may be turnover of existing customers after it is first disclosed. Then, there may be more enduring losses of potential customers after it is reported on by the media. Combined, these factors led to an average of $4.13 million in lost business for organizations affected by a data breach this past year.[4]

Finally, once the combined effects of operational, financial, legal/regulatory, and reputational consequences have shaken your business, the ability to reach your organization's short- and long-term strategic objectives will have been severely compromised.

OVERCOMING REAL AND PERCEIVED BARRIERS TO EFFECTIVE CYBERSECURITY

Every organization should have a comprehensive cybersecurity program. But, before you dive into developing a new or improved program, it is important to first recognize and overcome barriers to implementing successful cybersecurity measures.

Following are three of today's most common barriers.

While competing budget priorities may cause some to resist cybersecurity investments, overcoming this barrier requires a simple consideration: what is the cost of inaction?

1. Competing Business and Budgeting Priorities

Often the most immediate barrier is executive resistance due to competing business and budgeting priorities.

Unlike activities that overtly drive revenue growth, such as sales initiatives and service improvements, cybersecurity measures aren't exciting or enticing. Further, if a data breach has yet to affect your organization, there may be a lack of urgency for new or expanded cybersecurity investments.

Even when there is high-level concern for cybersecurity, organizations are often overwhelmed by the associated logistic and in-house resource challenges.

Many organizations struggle with fundamental technology operations, particularly those directly aligned with revenue generation. So, when cybersecurity requires complex tasks such as examining and addressing vulnerabilities in your software, applications, and mobile devices, it is easy to see how they can be avoided or deprioritized.

To overcome this barrier, it is important to convey the costs of action versus inaction.

The costs of inaction can be stunning and unpredictable. Remember: data breaches cost the average mid-sized company more than $9.5 million in 2017, with individual costs ranging wildly based on the size, type, and frequency of breaches.

Conversely, technology research firm Gartner estimates that companies employing effective, up-to-date cybersecurity measures dedicate 4 to 7 percent of their technology budget to security.[5] Based on the math alone, action is always preferable to inaction.[6]

2. Continually Shifting Threats and Trends

In addition to the challenge of getting cybersecurity classified as a key budget priority, many organizations face barriers in ensuring that their security measures, including training, processes, and technology, keep pace with emerging threats.

THREAT	POTENTIAL SECURITY ISSUES
Ransomware	While most security incidents are still due to phishing attacks, the volume of daily ransomware attacks has risen by 300 percent—to more than 4,000—from just two years ago.[7]
Mobile	Though mobile technology allows for access to information anywhere, anytime, it has also greatly expanded the number of potential points of compromise and unauthorized data access.
IoT	Since IoT is essentially digitizing analog objects (e.g., machinery, clothing, furniture), it is also making those objects prone to being compromised.

For instance, ransomware, mobile devices, the Internet of Things (IoT), and other developments are presenting new and difficult security issues. In fact, most (56 percent) of executives say that mobile devices and IoT are now the most vulnerable endpoints of their organization's networks and enterprise systems.[1]

[5]Source: 2016 Gartner Identifying the Real Information Security Budget Report.

[6]Note: These figures are provided solely for purposes of comparison, as technology spend alone is not an indicator of security effectiveness. The quality of expenditures is more important, and cybersecurity is reliant on many activities not related to technology budget. An independent advisor can recommend the appropriate spend levels for your organization.

[7]Source: 2017 U.S. Department of Justice Protecting Your Networks from Ransomware Report.

Given the complexity and changing nature of these threats, overcoming them requires a comprehensive, ever-evolving cybersecurity program—including the ongoing guidance of a technology advisor with broad cybersecurity expertise.

3. Your Biggest Threat: People

The last threat we'll discuss is also your biggest. Simply put, people are your organization's ultimate wildcard and your main risk to data security.

Employee negligence is the root cause of more than half (54 percent) of data breaches.[1] Most often it comes in the form of complacency, such as when employees don't follow computer access protocols, or technology resources don't perform necessary patch management or basic firewall updates. Less often it comes in the form of an insider threat, when an employee purposely exposes the organization to malware.

In the end, the best control frameworks and technology solutions are useless if employees don't act appropriately. So, to overcome this barrier, your cybersecurity program must focus on operations as much as technology. In particular, it must establish and maintain proper policies and procedures for company systems and data handling.

Further, it must reinforce those policies and procedures via administrative controls and internal education. For example, consider the ever-present threat of phishing emails containing attachments with malware. Since just one faltering employee can compromise your system, ongoing training is invaluable.

SIX CORE COMPONENTS OF A COMPREHENSIVE CYBERSECURITY PROGRAM

Developing, implementing, and maintaining a comprehensive cybersecurity program is a difficult yet necessary effort, requiring organizations to shift their operations, strategies, and overall approach to security. Rather than a "one-and-done" activity, cybersecurity must be woven into your corporate culture and embraced by leadership.

With this level of commitment—and incorporation of the following six core components—organizations can establish a successful cybersecurity program that delivers dependability and long-term value.

1. **Defining and Identifying Your Valuable Information**

   Before implementing any new technology or procedures, it is critical that organizations define what constitutes "valuable" information.

   In lieu of labelling all data as valuable, this activity should identify only what assets need to be protected. Specificity is vital, as the protection of this information will serve as the foundation of your cybersecurity program.

2. **Employing Key Operational Management Processes**

   Among the most important activities for a successful cybersecurity program is the development of clear, detailed operational processes and strategies for managing risk and responding to cybersecurity incidents.

Contrary to popular belief, an effective cybersecurity program is more of a business operations effort than a technology effort—requiring processes and accountability for managing risk and responding to incidents.

Several agencies and organizations, such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS), provide baseline guidance for developing these measures. For example, NIST's Risk Management Framework outlines a process that includes:

- Categorization of information systems
- Selection of security controls
- Implementation of security controls
- Assessment of security controls
- Authorization of information systems
- Continuous monitoring of security controls and performance of diagnostics to identify problem areas

3. Providing Ongoing Training and Education

Since employees are the biggest threat to cybersecurity, organizations should provide continual education on cybersecurity policies and procedures via:

- Inclusion of cybersecurity content in onboarding, employee training, and operational processes
- Regular, organization-wide communications of cybersecurity-related information
- Ongoing reviews of internal procedures involving sensitive information

This effort is a key part of making cybersecurity a part of your corporate culture. As such, cybersecurity should be listed as a critical organizational objective and ingrained as part of every employee's professional development.

4. Implementing and Configuring the Proper Technology

Complementing your processes and procedures should be technology solutions appropriate for your organization's structure, size, security risks, and budget. Proper configuration and maintenance are essential to keep pace with evolving threats.

---

[8]Source: 2017 Hiscox Cyber Readiness Report.

5. Exploring and Purchasing Cyber Insurance

In conjunction with internal efforts, a comprehensive program should include cyber insurance to protect your organization. Though relatively new, cyber insurance is quickly becoming a standard part of corporate insurance portfolios. In fact, more than half (55 percent) of U.S. companies now carry some form of cyber insurance.[8]

To qualify for and obtain the appropriate types and levels of coverage, we recommend working with an independent technology advisor to quantify your organization's risk. This entails examining your computing environment, its areas of vulnerability, and where "valuable" data is located.

6. Establishing a Relationship with a Trusted Technology Advisor

Developing, implementing, and maintaining a comprehensive cybersecurity program is an important and complex task. So, while companies can develop their cybersecurity program internally, many are recognizing the benefits of engaging a specialized technology advisor.

In addition to helping you obtain cyber insurance, a technology- and vendor-agnostic advisor can serve as a valuable strategic partner, providing an independent, insightful perspective on your people, processes, and vulnerabilities.

Ultimately, with the ever-evolving nature of cybersecurity threats and practices, the right advisor can help you more effectively identify solutions that set your business up for success and dependability—both now and in the future.

CONTACT US

For More Information

To learn more about today's key cybersecurity challenges—and how to implement the right program for your organization—click here to contact SC&H Group's Technology Advisory Services team.

Jeff Bathurst
Director
- 410-785-8835
- jbathurst@schgroup.com

Chris Rossi
Principal
- 410-785-8587
- crossi@schgroup.com

Greg Tselikis
Principal
- 410-988-1389
- gtselikis@schgroup.com

About SC&H Group

SC&H Group is a nationally recognized management consulting, audit, and tax firm serving clients from rapidly growing private sector businesses to Fortune 500 companies with global brands. The firm's strategic practices provide the leading-edge thinking and advice that transform our clients' businesses and help them outpace the competition. We embrace the future and help clients prepare, innovate, and evolve their businesses in this complex and highly competitive world. For more than 25 years, SC&H Group has demonstrated its commitment to delivering powerful minds, passionate teams, and proven results on each and every engagement. To learn more visit www.schgroup.com.