



Secure
the Holidays



Hello,

The holidays are a time to focus on the truly important things in life – family, friends, and giving selflessly to others. But we cannot extend our generosity to cybercriminals by leaving valuable data and information vulnerable to attack, even while we take time away from work.

In this playbook we share not only the vital building blocks for a compliant security posture, but unwrap some of the nefarious schemes hackers use and deliver tactics your business can apply all year round.

We extend to you the gift of compliant security strategies every organization can implement today and are here to fill in any gaps that you might find along the way.

Sincerely,

Team Ntirety

Table of Contents

PAGE

04

Five aspects of
cybersecurity

PAGE

08

Identification

PAGE

11

Protection

PAGE

13

Detection

PAGE

19

Response

PAGE

22

Recovery

PAGE

24

Stack Your Cybersecurity
Snowman

PAGE

BC

About Ntirety



Click on logo to go back to TOC



Five aspects of Cybersecurity

Wrapped up for the Holidays

Cybercriminals do not take a break on weekends, nights, or holidays. Protecting business IT and maintaining compliance should be a top priority year-round, but the winter season presents ample distractions for businesses that turn into tempting opportunities for hackers to swoop in under the radar and wreak havoc.

While strong cybersecurity may be on the company wish list, a truly compliant and secure IT environment is more like assembling a gingerbread house rather than one solution wrapped up with a bow. Businesses need to start with a sturdy foundation across the organization, layer a framework on top of it, and pay attention to all of the details.



1 Identification

Internal IT visibility is the core component necessary for swift and accurate identification of issues, threats, and compliance requirement violations. Organizations must understand their environment in order to manage cybersecurity risk to systems, assets, data and capabilities, including preventative measures such as routine patching and monitoring and compliance audits. In addition, it is crucial to research and regularly familiarize teams with the main types of cybercrime and how they're perpetrated, like phishing and ransomware as well as those that could be coming from within.

2 Protection

Developing and implementing the appropriate safeguards to limit or contain the impact of a potential cybersecurity event is critical to every security plan – including governance for internal teams. To comply, organizations must:

- Control access to digital and physical assets
- Provide awareness education and training
- Create processes to secure data, and
- Maintain documentation that satisfies any required compliance measures



Five aspects of Cybersecurity

3 Detection

An effective threat detection strategy requires an investment in compliant security tools, training and retention of skilled employees, or outsourcing support to fill the gaps. Blending both technology and human teams presents a challenge on a variety of levels for businesses, but striking a balance is imperative to a proactive and compliant security posture.

4 Response

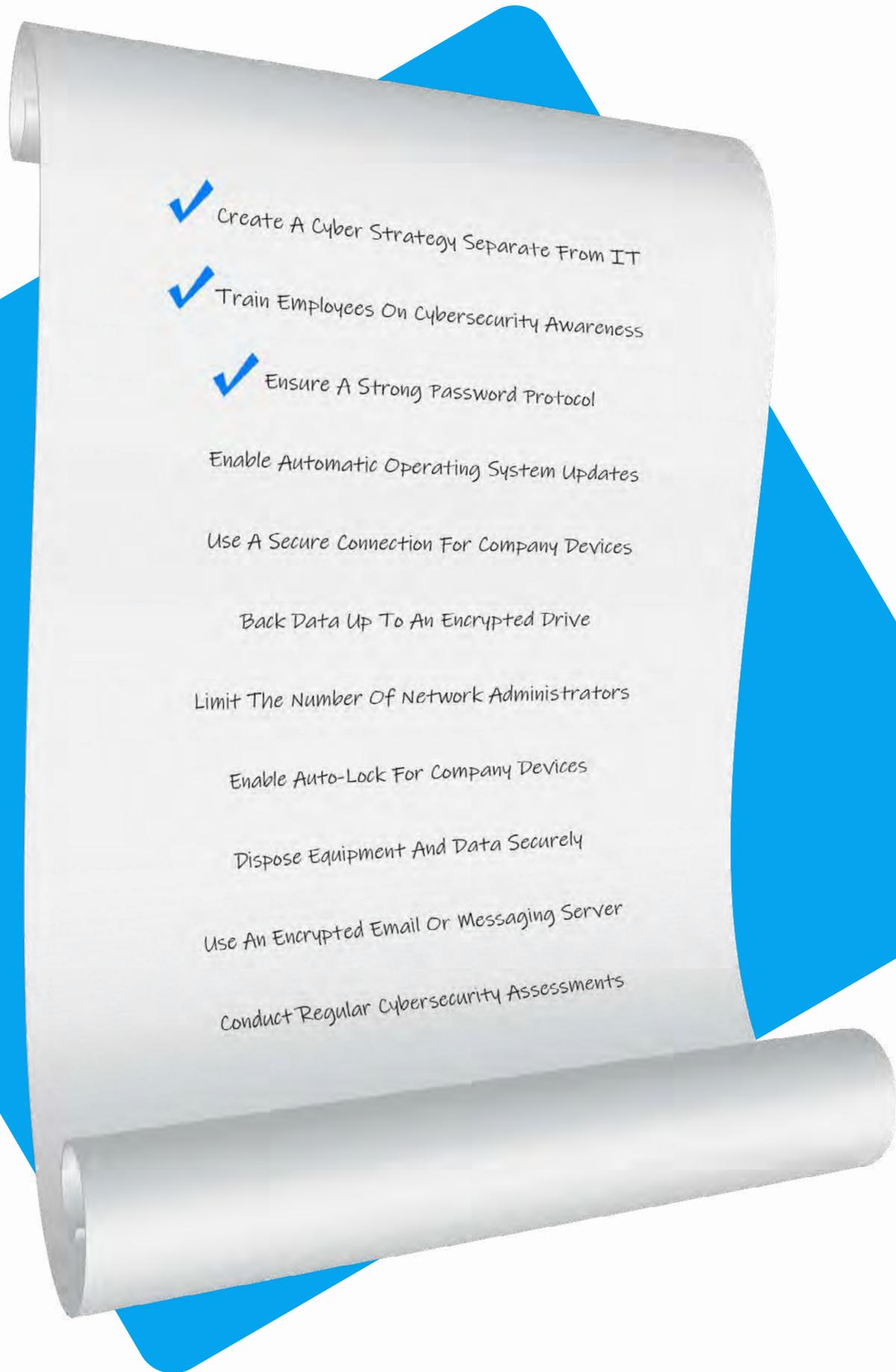
Organizations must have the ability to contain the impact of any cybersecurity incidents and be prepared with an internal and external communications plan. To create a solid response plan, internal stakeholders must define communication lines, collect and analyze information about the event, perform all required activities to eradicate the issue and incorporate lessons learned into revised response strategies – no small order when it comes to the ever-growing variety of IT risks.



5 Recovery

Organizations must develop and implement effective activities to restore any capabilities, services, and compliance measures that were affected due to a cybersecurity event. A recovery plan must be in place to coordinate restoration activities with external parties and incorporate lessons learned into your updated recovery strategy. Defining a prioritized list of action points and routinely testing the plan are critical for a timely recovery.

The average time to identify and contain a data breach is **280 Days** and costs organizations an average total cost of **\$3.86M¹**

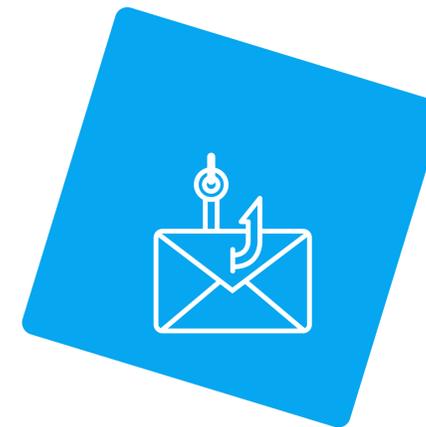


- ✓ Create A Cyber Strategy Separate From IT
- ✓ Train Employees On Cybersecurity Awareness
- ✓ Ensure A Strong Password Protocol
- Enable Automatic Operating System Updates
- Use A Secure Connection For Company Devices
- Back Data Up To An Encrypted Drive
- Limit The Number Of Network Administrators
- Enable Auto-Lock For Company Devices
- Dispose Equipment And Data Securely
- Use An Encrypted Email Or Messaging Server
- Conduct Regular Cybersecurity Assessments

Identification

Make a List, Check It Twice

To identify cyberthreats, teams across the organization must be able to recognize the risks that come with technology – from opening email to skipping IT patches and using work devices at home, employees should be educated on safe practices and due diligence.



Phishing

Today hackers have more subtle and sophisticated techniques for stealing data than most organizations may realize. Phishing, or the fraudulent practice of sending emails that look to be from reputable companies, is at the top of the list for hackers. Phishing is the number one type of social engineering attack, accounting for more than 80 percent of reported incidents².



Ransomware

WannaCry, CryptoLocker, Jigsaw, Petya – there are many names for the variant strains of ransomware, but at their core they all threaten to publish the victim’s data or perpetually block access to it unless a ransom is paid. Despite the funny names of these attacks, the ransoms are no laughing matter. The United States alone has seen a ransomware attack increase of nearly 200% in the past two years. The cost to recover data from the cybercriminals, now averages more than \$100,000³.



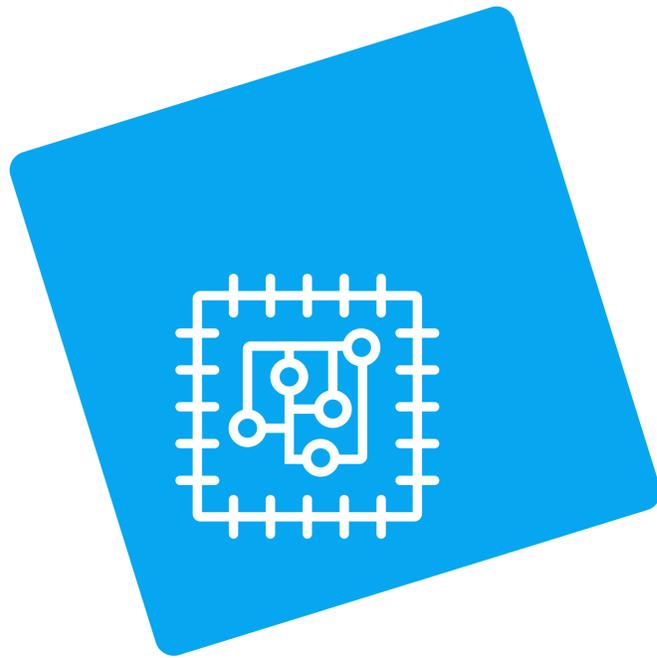
Compliance Requirements

CCPA, PCI, HIPAA and GDPR are just a few of the various compliance regulations that organizations can be affected by – and penalized for failing to meet the standards. Having a solid understanding of the requirements can be just as challenging as actually meeting them since they frequently change and new regulations are being introduced at record rates.



Remote Work & BYOD

How familiar are your remote work teams with the security and compliance protocols that go along with using virtual desktops (VDI), virtual private networks (VPN), and “bring your own device” (BYOD) practices? Surveys of remote workers using BYOD policies over the past year have found nearly 25% of employees working from home do not know what security protocols are in place on their device⁴. If that number is not unsettling enough, organizations utilizing remote work more than half of the time took an average of 316 days to identify and contain a data breach. For organizations less than 50% it took 258 days⁵.



Patching

A patch is a set of changes to an IT program or its supporting data designed to update, fix, or improve it, and are sometimes referred to as bug fixes. IT and security teams spend much of their team resolving issues set in place because of failed patches (19%)⁶. The rest of the time is spent testing patches (15%) and coordinating with other departments (10%). The patching challenges for IT and Cybersecurity professionals may be the reason 49% of respondents to a recent survey believe their company's current patch management protocols fail to effectively mitigate risk.



Identifying these risks is the first step towards a solid compliant security posture. Without an understanding of the threats in today's technology landscape, a business is left vulnerable.

Firewalls

A firewall is the system designed to be a barrier between your IT network and incoming traffic in order to block malicious traffic like viruses and hackers. But that basic traditional firewall that everyone is familiar with is just that – basic. In survey of over 250 black hat hackers, 73% said traditional firewall security is irrelevant or obsolete⁷. A basic firewall will block traffic deemed dangerous, but if a user clicks on a phishing email or is connected to a compromised VPN then hackers can stroll past that firewall.



Monitoring

Monitoring tools and software are the eyes and ears keeping track of an IT environment and ensuring equipment is performing as expected – but the human element is still needed to be the boots on the ground in case anything goes awry. This balance of IT tools and team members is what makes monitoring a struggle for many companies and creates a high security risk. Lack of visibility into all parts of IT environments, the increasing complexity of systems, and the sheer volume of data and applications all put a strain on the human eyes, ears, and minds trying to monitor, analyze, and mitigate threats.

Protection

Could the Grinch Come from Within?

Protecting an organization's IT infrastructure and applications and maintaining compliance come as the natural next step after identifying the top risks, yet research shows that businesses are still unprepared when it comes to even the most common risks that threaten data and compliance.

35% 37% 38%

Phishing is the most common action that initiates a data breach⁸

of organizations were hit with ransomware in the last year⁹

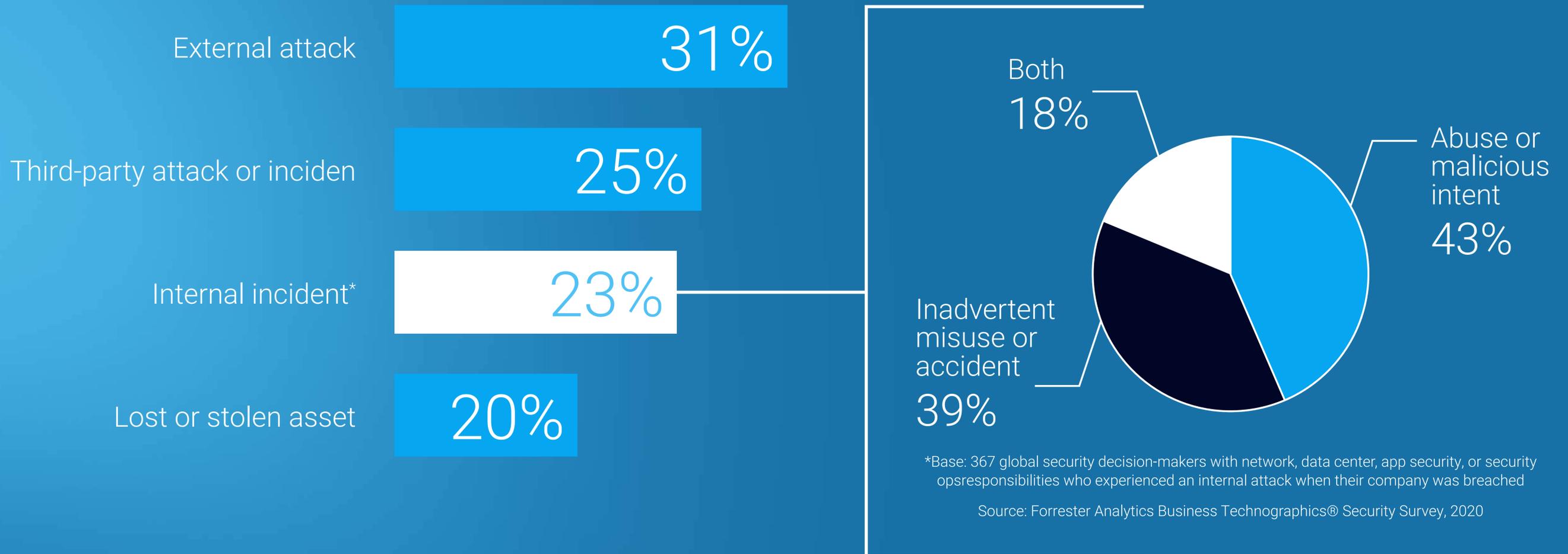
of causes for a data breach are Employee carelessness accounts¹⁰

While most companies are at least aware that there are a variety of outsider threats to their IT systems, defending against internal incidents ranks third in types of attacks a business faces. 43% of these internal threats are malicious insiders¹¹. Just as ransomware strains can take many different names as we saw above, insider threats can come from a much wider range of individuals than just employees with high access levels.



Percentage of Respondents Who Experienced Attacks

Least one of the following types of attack in the past 12 months



Looking past the holidays into strategies for the new year, increased focus on IT governance within organizations is needed for stronger security. In addition to understanding outsider threats, visibility and control over internal user access stand out as key elements to bridging identification with protection and lead into effective threat detection.



Detection

Automate, Upskill, and
Outsource – No Elves Needed

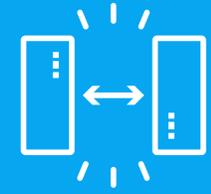
A three-pronged approach to threat detection is recommended:



Serious investments in compliant security tools and teams



Training and retention of skilled tech employees



Outsourcing for support to fill the gaps

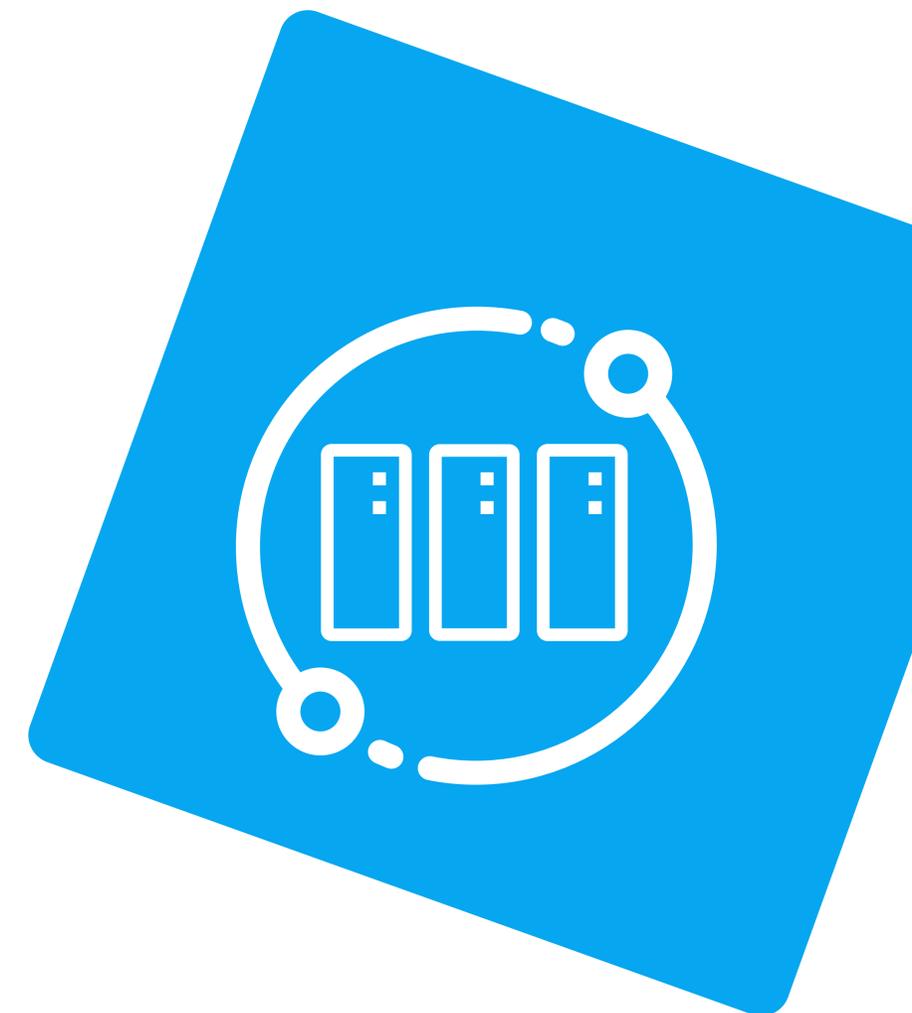
This strategy enables businesses to embrace the changing landscape and invest in their internal talent while simultaneously leveraging outside resources.

Tools & Teams

The coordination, tuning, and orchestration of various tools for the necessary 24x7 visibility of an IT environment is most effective with a Security Operation Center (SOC) to implement and ensure strong, compliant cybersecurity.

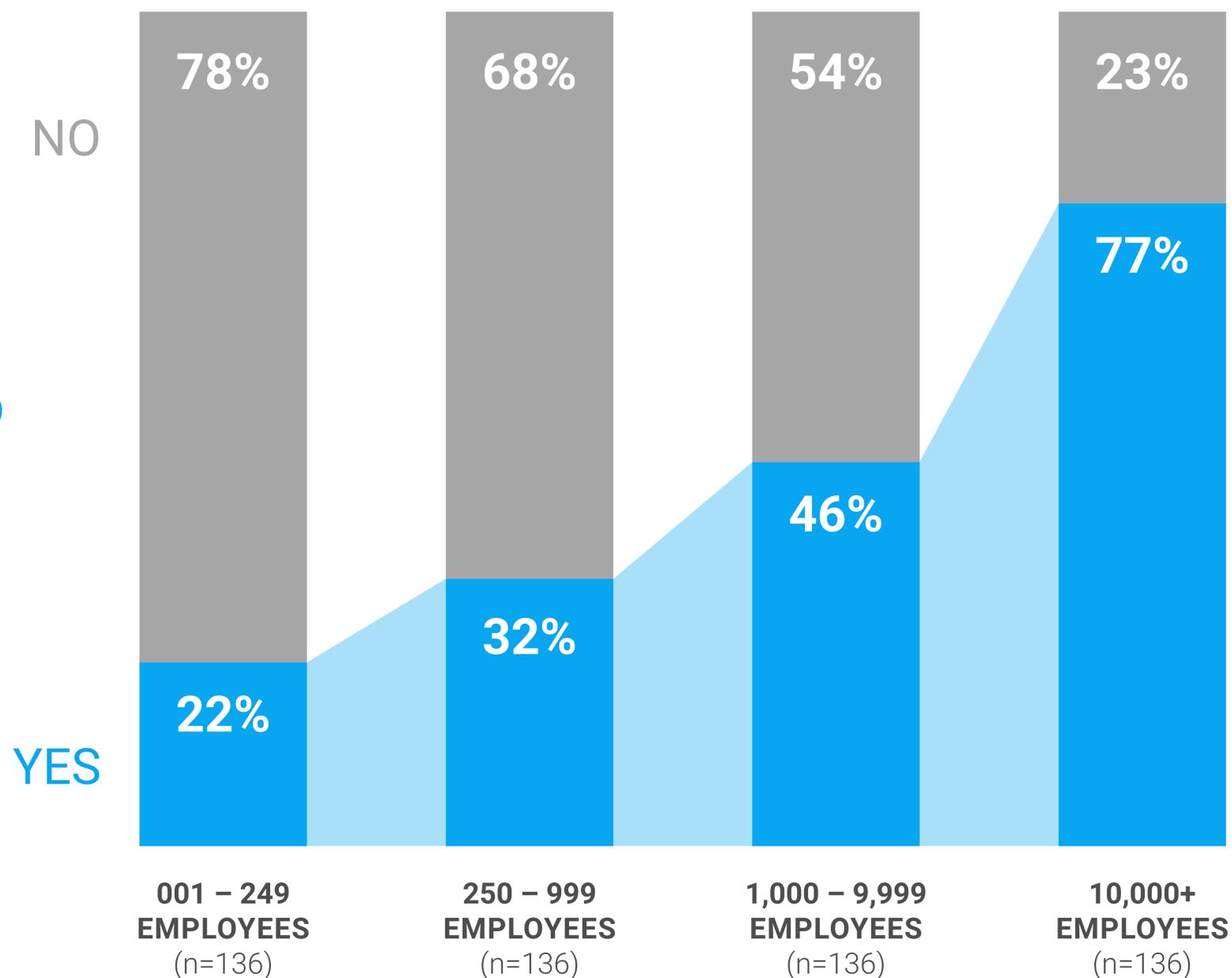
The operational needs of a SOC are generally more sophisticated, requiring a Security Information and Event Management platform (SIEM). This well-established security monitoring system, along with firewalls, and intrusion detection/prevention (IDS/IPS), are some of the most important tools in an SOC. Additional security measures, such as email filtering, log review, and user behavioral analytics, can bolster a cybersecurity team by automating some of the necessary monitoring and defense responses.

Having a SOC in place is most common with larger organizations that assumably have the bandwidth and budget to bring experts on board to implement and operate modern cybersecurity tools and technologies.



The Presence of a SOC Aligns Closely to Organizational Size

SOC in Place?



For companies that may not be able to recruit or retain security experts long-term, training existing teams is a worthwhile investment that can be a cost-effective strategy.



Internal Training & Skills Development

The core question organizations should ask themselves when it comes to threat detection is not about what tools or platforms to use, but rather the human element:

Does your staff have in-house information security and risk management expertise?

Security Staffing Pressure Continues Unabated as IT Architecture Becomes More Complex

Information Security Snapshot



State their organization **do not have enough information security personnel**



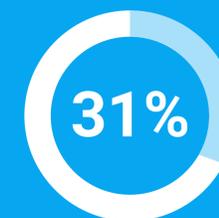
Do not believe their security staffing level is adequate to handle the challenges faced by their organizations



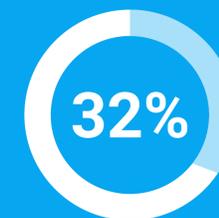
Rate **recruiting** information security professionals as **significantly difficult**



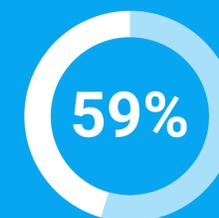
Of organizations have **dedicated security leadership in place**



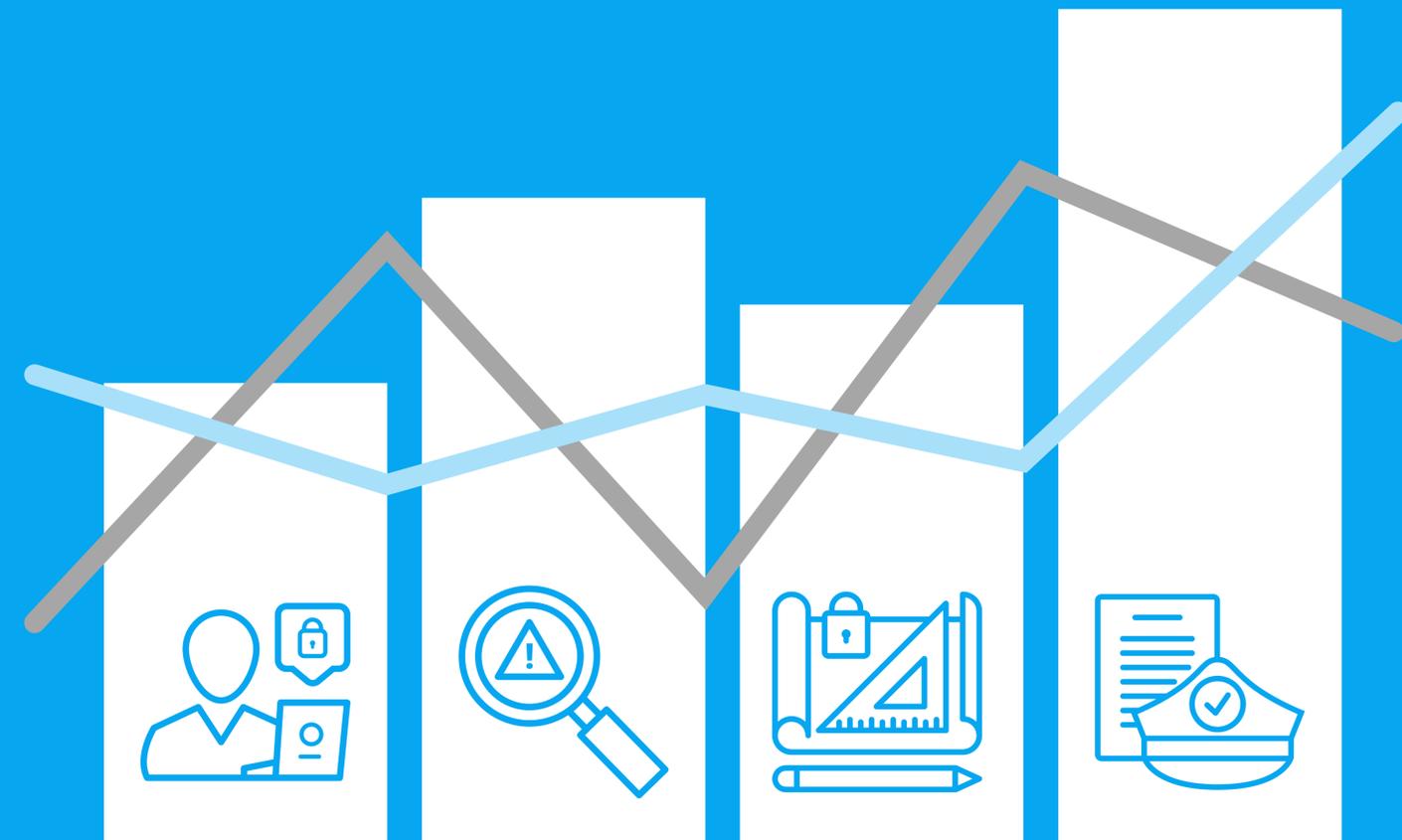
Believe the head of information security is **not well positioned to effect cultural change**



Rate **retaining** information security professionals as **significantly difficult**



Project salaries for security professionals will **rise in the next 12 months**



Finding the personnel to fill advanced positions like Security Analyst, Threat Researcher, Security Architect, or Compliance Officer is an increasing challenge for organizations of all sizes across industries. The overall talent market has a noticeable shortage of advanced cybersecurity skills, and there are not enough resources across the board.

With this ongoing cybersecurity talent drought, businesses must make a serious investment in the training and retention of skilled tech employees. While these programs take time to set up, the industry is witnessing positive pushes to manage workloads and advance technologies in critical situations via training programs that aim to upskill existing talent.

Upskill

The practice known as "upskilling" is the process of teaching current employees new skills to minimize talent gaps¹². With thousands of new product and feature releases per cloud platform and new compliance regulations emerging each year, tuning up and updating cloud skills is essential to employee success. Another often overlooked benefit of upskilling is that it creates a positive culture of learning in the organization.

Even with training and efforts to retain current staff, the realities of the talent and skills shortage are often best resolved by outsourcing critical IT skills to a trusted compliant security partner.

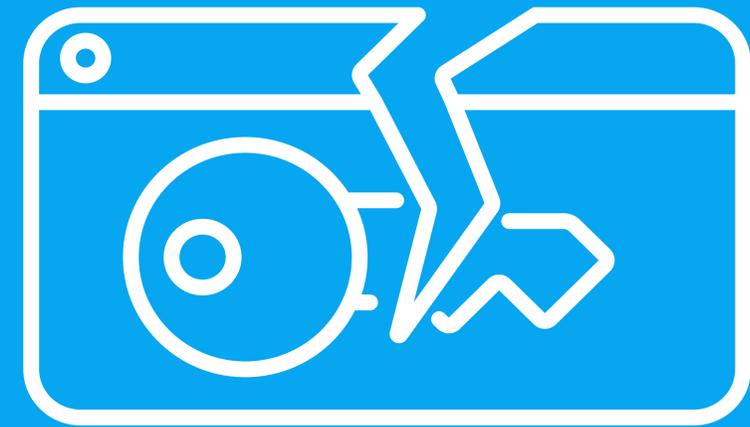


Third-Party Support & Outsourcing

The demands of a strong compliant security posture are high, and organizations that are not able to operate an in-house SOC 24x7 must find ways to ensure their security and compliance standards are not waning.

Outsourcing aims to act as a seamless extension of the internal IT team. Businesses are able to leverage outside firms who specialize in Compliant Security as a Service, helping an organization achieve the 24x7 monitoring and routine compliance auditing.

While finding the right partner includes evaluating the skills and services they offer, businesses must also ask themselves the question:



Are you assessing third-party and vendor risks and threats?

Third-party vendors have been the source of massive data breaches, including incidents with Quest Diagnostics, Marriott Hotels, General Electric, and the list goes on. Supply chain risk and assessment is a critical component to prevent security breach or crisis and continue to meet compliance regulations. Vendor assessments can be time consuming and difficult to track, but putting processes in place to evaluate can make it easier and repeatable. Ensuring that all risks are identified and scored is a key indication of a mature risk program ready to safely partner with a third-party.

Response

24x7x365 Season's Greetings



When a threat is detected or a cyber-crisis rapidly unfolds, sounding the alarm for quick response requires its own plans and preparations. Who, what, when, where – these aren't just questions to answer about an incident, but considerations when developing a communication plan.



Key Considerations for Constructing a Communication Plan

Identify & Prep a Cyber-Crisis Team

For an incident involving IT security, the right individuals within the organization must be prepared to respond. Along with the CEO and CFO, the team should include the Chief Information Security Officer (CISO) or highest-ranking IT employee, as well as key people from public relations, corporate communications, investor relations, and human resources.

Develop & Distribute the Messaging Plan

Developing a basic messaging “template” related to the most probable risks will help the crisis team to be prepared to swiftly communicate if a successful attack ever occurs. Along with tailoring the messaging to address the nuances of the actual crisis, the public communications must always include a mitigation plan. Know who has been affected and to what extent.

Set Messaging Timeline

In conjunction with determining the messaging, develop a timeline to announce the incident - but be sure to expect the unexpected. Try to anticipate various scenarios and how they could affect the message you send. Determining the cause and all the ripple effects of a cybersecurity crisis can take months, but companies are still accountable in the public eye even if they do not have all the answers.

Know your Stakeholders

Important beyond crisis communications, it should be a foundational practice to maintain the current contact information of all of an organization's major stakeholders. Not just email addresses and phone numbers, but knowing the people. A good, established relationship with stakeholders makes delivering news easier, especially if that news is hard to digest. Establishing these relationships should also build confidence with clients that the right team and plan in place if a security incident occurs.

Remember the Role of the Board

The SEC expects boards to be aware of their companies' cybersecurity policies and procedures. While the board does not need to be heavily involved in the crisis communication planning process, it should be aware of messaging and response plans in case a cyber crisis should arise.



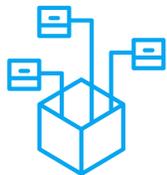
Recovery: Be Prepared There's No Gift Receipt for a Data Breach

A disaster will hit your organizations—it's only a matter of time. Business interruptions from natural disasters, vendor breaches, and ransomware make business continuity mission-critical for organizations to proactively safeguard against lost data and downtime. Going beyond availability, business continuity plans determine how your business will continue to run and maintain compliance standards as best as possible in times of trouble.



Geoclustering

This allows businesses to simulate or perform failovers to remote sites on a simulated or actual basis at any time of the day or night.



Logistics Testing

This should be performed two to four times a year, plus following significant changes to business processes or infrastructure.



Tabletop Exercises & Plan Walkthroughs

These testing methods can be used much more frequently than formal off-site tests, are less expensive to conduct with fewer logistical requirements, and allow teams to interact through the documented procedures.

What are your Recovery Time and Point Objective RTO/RPO?

Recovery Time Objective (RTO):

As you build your disaster recovery strategy, you must make two crucial determinations. First, figure out how much time you can afford to wait while your infrastructure works to get back up and running after a disaster. This number will be your RTO. Some businesses can only survive without a specific IT system for a few minutes. Others can tolerate a wait of an hour, a day, or a week. It all depends on the objectives of your business.

Recovery Point Objective (RPO):

The second determination an organization must make as they discuss disaster recovery is how much tolerance they have for losing data. For example, if your system goes down, can your business still operate if the data you recover is a week old? Perhaps you can only tolerate a data loss of a few days or hours. This figure will be your RPO.

While the goal of every security strategy should be to prevent a cyber-crisis from occurring, the best plans include disaster recovery and business continuity. Taking a proactive stance towards recovery drills is an additional layer of strength to a compliant security plan.



Stack Your Cybersecurity Snowman

Individual snowflakes are easily tossed around in the wind, but when packed together with the right plan, a solid snowman can form that will stand tall through wintry weather. Similarly, individual IT security tools and practices implemented alone can easily be bypassed by cybercriminals, but combined together in the right strategy, a strong cybersecurity posture will form that will stand up to cyberthreats.



Top – Response & Recovery

Three round spheres of snow are the foundational elements, just like identification, protections, and detection are the core of every cybersecurity strategy, but the corn cob pipe, button nose, and two eyes made out of coal mean no second glances are needed to recognize a snowman. Response and recovery plans are key to conveying all the aspects of a security strategy quickly and easily.

Middle – Protection & Detection

The middle section is where your snowman – and your security strategy – really starts to take shape. The protection and detection plans turn understanding into action, just like the middle of a snowman transforms what otherwise would just be a pile of snow into a familiar shape.

Bottom – Identification

The base of any snowman must be the biggest to balance all of the elements. Just like thousands of snowflakes are rolled together to make a solid support, a strong security posture starts with a comprehensive base of identifying risks, threats, and vulnerabilities to adequately set up protection, detection, response, and recovery plans.

Ntirety delivers compliant security solutions that cover the entire application, the entire compliance and security process, the entire time.

A leader in delivering secure managed hybrid and multi-cloud solutions to more than 2,500 enterprise customers around the globe, enables businesses to shift from managing operational risk to creating a future-ready, agile enterprise.

Ntirety's compliant managed cloud and cybersecurity services are supported by over 500 top technical certifications and the industry's first Guidance Level Agreements (GLAs). Offered only by Ntirety, GLAs go above and beyond expectations set by SLAs, keeping clients a step ahead of the competition with actionable recommendations that enable better business outcomes.

© 2021 Ntirety, Inc. All Rights Reserved. Ntirety is registered trademark of Ntirety, Inc. All trademarks, logos and brand names are the property of their respective owners.

Sources:

1. [IMB Cost of a Data Breach Report, 2020](#)
2. [2021 Data Breach Investigations Report](#)
3. [2021 State of Ransomware Survey and Report](#)
4. [2020 WFH EMPLOYEE CYBERSECURITY THREAT INDEX](#)
5. [Cost of a Data Breach Report 2021](#)
6. [Ivanti Patch Management Challenges](#)
7. [Bitglass 2020 BYOD Report](#)
8. [2021 Data Breach Investigations Report](#)
9. [State of Ransomware 2021](#)
10. [Code42 2021 Data Exposure Report](#)
11. [Best Practices: Mitigating Insider Threat](#)
12. [Forbes 2019: As The End Of 2020 Approaches, The Cybersecurity Talent Drought Gets Worse](#)