Cybersecurity Playbook

Ntirety

Hello,

It is an understatement to say that the business landscape has simply changed — the upheaval brought on by the pandemic, shifting to a remote workforce, economic instability, online education, greater scrutiny on tech giants, and the list goes on. Organizations are now facing new challenges, greater uncertainty, and heightened cybersecurity risks.

With all these changes, organizations are more vulnerable than ever to opportunistic cybercriminals taking advantage of this new world. Hackers are opening their cybercrime toolboxes — and organizations need to be better prepared.

This playbook contains not only the vital building blocks for a compliant security posture, but also unveils some of the nefarious schemes hackers use and includes tactics you can implement to better protect your organization.

Thank you,

Emil Sayegh

Chief Executive Officer, Ntirety

TABLE OF CONTENTS

Five Aspects of Compliant Cybersecurity

Cybercriminals do not take a break on weekends, nights, or holidays. While protecting business IT should be a top priority for companies 24/7/365, resource limitations and unexpected distractions pulling away a company's attention can turn into tempting opportunities for hackers to swoop in under the radar and wreak havoc.

Combatting cybercriminals takes more than an out-of-the-box solution or hiring extra hands to cover off-hours. Developing a truly secure IT environment is more like assembling a house — start with a sturdy foundation across the company, build a framework and layers on top of it, and pay attention to all the details that make a fortress in order to intimidate bad actors and impress stakeholders.

Five Aspects of Compliant Cybersecurity

Identification

Internal IT visibility is the core component necessary for swift and accurate identification of issues, threats, and compliance requirement violations. Businesses 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.

Five Aspects of Compliant Cybersecurity

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, businesses must:

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

Five Aspects of Compliant Cybersecurity

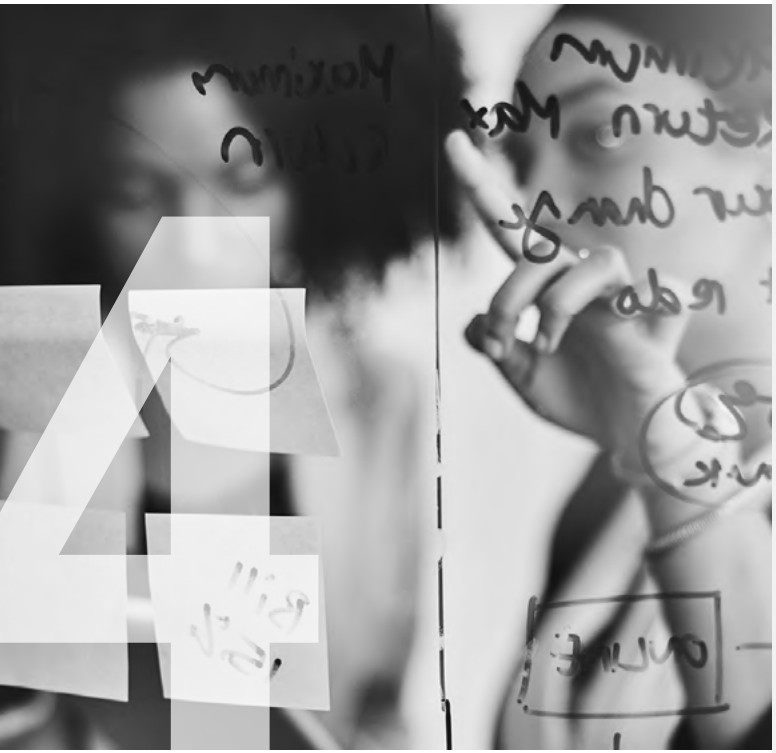
Detection

An effective threat detection strategy requires an investment in compliant security tools, training, and retention of skilled employees, or outsourcing support in order 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.

60% of security professionals say the cybersecurity skills shortage has a negative impact on incident detection and response.

Source: Cybersecurity Skills Gap Survey 2019

Five Aspects of Compliant Cybersecurity



Response

Businesses must have the ability to contain the impact of any cybersecurity incidents and be prepared with an internal and external communications plan. An IT team is expected 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. This is no small order when it comes to the ever-growing variety of IT risks.

Five Aspects of Compliant Cybersecurity

Recovery

Businesses must develop and implement effective activities in order 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 an 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 businesses an average total cost of** $3.68M.[1]

Identification

Risks, Regulations, and Required Safeguards

Identification

To identify cyberthreats, teams across the business must be able to recognize the risks that come with technology — from opening email to skipping IT patches to 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 businesses 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% of reported incidents.[2]

Ransomware

WannaCry, CryptoLocker, Jigsaw, Petya — there are many names for the various 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. While the cost of these attacks today may make your jaw drop, surpassing $7.5 billion, **they are estimated to jump up to $21 billion**.[3]

Compliance Requirements

CCPA, PCI, HIPAA, and GDPR are just a few of the various compliance regulations that businesses 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 and 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 that nearly **25% of employees working from home do not know what security protocols are in place on their devices**.[4] If that number is not unsettling enough, one in four businesses have fallen victim to malware that workers downloaded to their personal devices.[5]

Patching

A patch is a set of changes to an IT program or its supporting data designed to update, fix, or improve it, and is sometimes referred to as a bug fix. But **60% of data breaches are linked to an IT vulnerability** where a patch was available but not applied.[6] Although patches are an essential part of preventative maintenance to keep IT systems up to date and safe, businesses delay patching for a variety of reasons ranging from a lack of resources (77%) to difficulty prioritizing patching (72%) to admitting that it simply slips through the cracks (56%).

Firewalls

A firewall is the system designed to be a barrier between an 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 a survey of over 250 black hat hackers, **73% said traditional firewall security is irrelevant or obsolete**.[7] 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. The need for a 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.

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

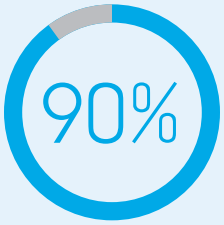
Protection

From the Inside Out

Protection

Protecting a business's IT infrastructure and applications and maintaining compliance come as the natural next steps 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.

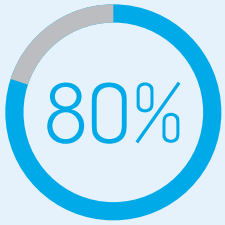
While most companies are at least aware that there are a variety of outsider threats to their IT systems, defending against malicious insiders ranks second in the risks businesses are least prepared for.[11] Just as ransomware strains can take many different names as we outlined above, insider threats can come from a much wider range of individuals than just employees with high access levels.



of cyberattacks that lead to a data breach begin with a phishing email.[8]

Estimates show that a business will fall victim to a ransomware attack every

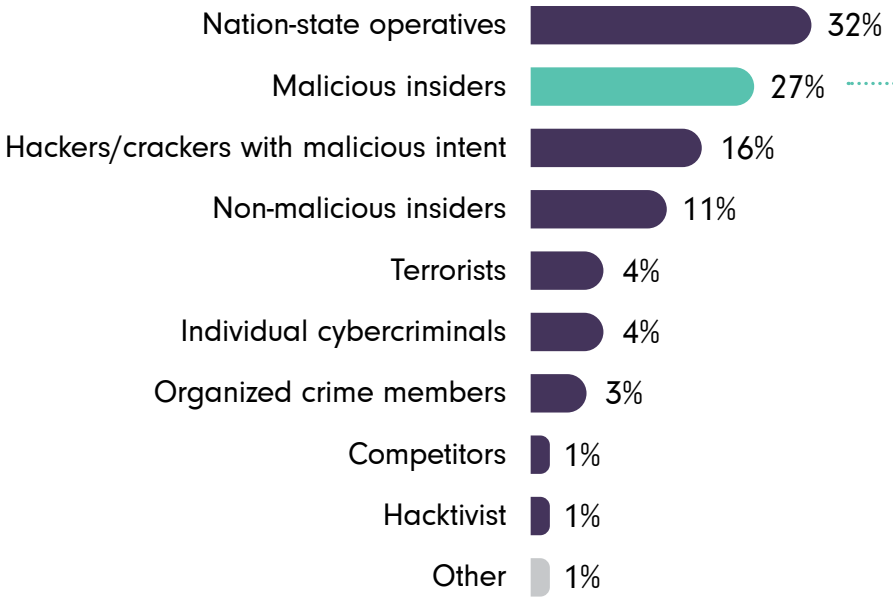
14 seconds.[9]



of breaches are caused by employee carelessness.[10]

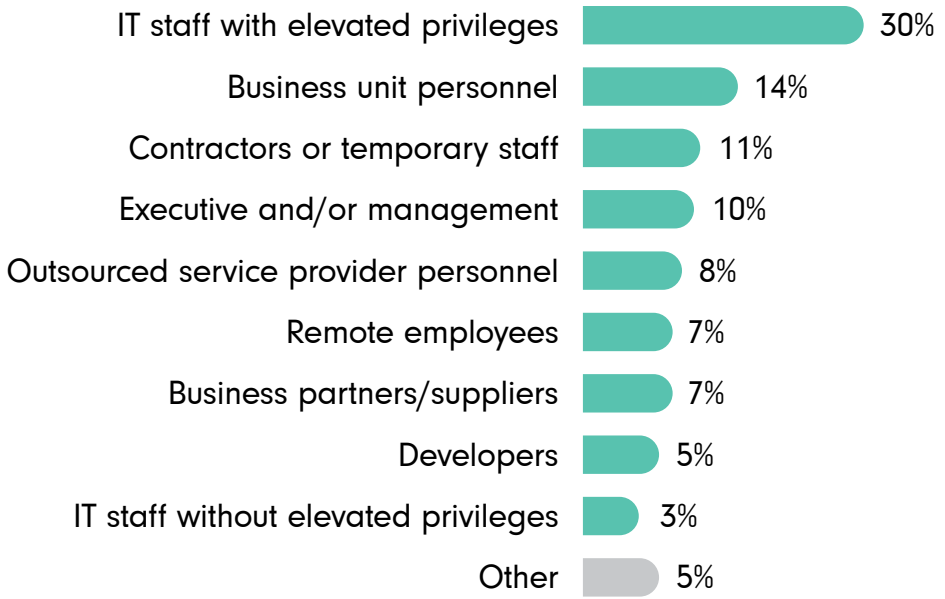
Threats Least Prepared For

Percentage of respondents, abbreviated fielding (n=139)



Primary Insider Threat Risks

Percentage of respondents, abbreviated fielding (n=154)



Overall, increased focus on IT governance within businesses 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

Detection

A three-pronged approach to threat detection is recommended:

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

1

Tools and Teams

Serious investments in compliance and security tools and teams

2

Internal Training and Skills Development

Training and retention of skilled tech employees

3

Third-Party Support and Outsourcing

Outsourcing for support in order to fill the gaps

Tools and Teams

The coordination, tuning, and orchestration of various tools for the necessary 24/7 visibility of an IT environment are most effective with a Security Operation Center (SOC) to implement and ensure strong, compliant cybersecurity.

The operational needs of an 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 an SOC in place is most common with larger businesses that assumably have the bandwidth and budget to bring experts on board to implement and operate modern cybersecurity tools and technologies.

The Presence of an SOC Aligns Closely with Organizational Size

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.

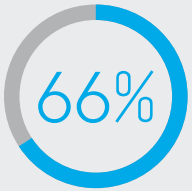
Internal Training and Skills Development

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

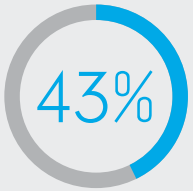
Does your staff have in-house information security and risk management expertise?

Security Staffing Pressure Continues Unabated as IT Architecture Becomes More Complex

INFORMATION SECURITY SNAPSHOT



state their organizations **do not have enough information security personnel**



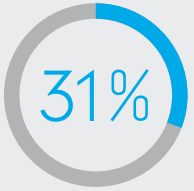
rate recruiting information security professionals as **significantly difficult**

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

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

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

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



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

Finding the personnel to fill advanced positions like security analyst, threat researcher, security architect, or compliance officer is an increasing challenge for businesses 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 in order to minimize talent gaps.[12] 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 business.

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 and Outsourcing

The demands of a strong compliance and security posture are high, and businesses that are not able to operate an in-house SOC 24/7 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 that specialize in Compliant Security as a Service, helping a business achieve 24/7 monitoring and routine compliance auditing.

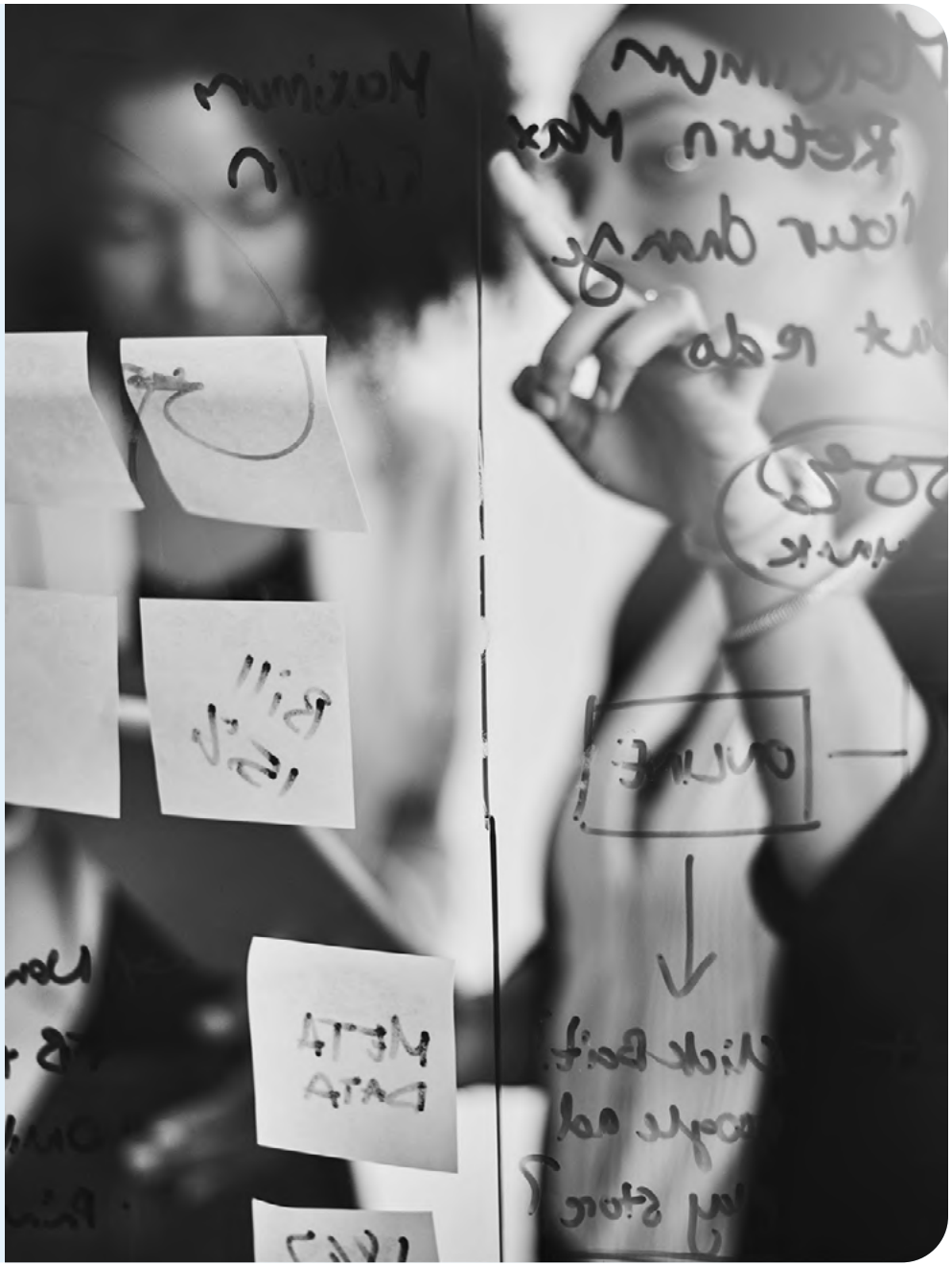
While finding the right partner includes evaluating the skills and services they offer, businesses must also ask themselves the question:

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, and General Electric. Supply chain risk and assessment is a critical component to preventing security breaches or crises and continuing 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

Clear Communications Across Audiences



Response

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

Key Considerations for Constructing a Communication Plan

Identify and Prep for a Cyber Crisis

For an incident involving IT security, the right individuals within the business 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 and Distribute the Messaging Plan

Developing a basic messaging "template" related to the most probable risks will help the crisis team be prepared to swiftly communicate if a successful attack ever occurs. Along with tailoring the messaging to address the nuances of the actual crisis, public communications must always include a mitigation plan, including details about 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

Beyond crisis communications, it should be a foundational practice to maintain the current contact information of all of a business's major stakeholders. This is 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 are in place when 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 a 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,
Be Resilient —
With Business Continuity

Recovery

A disaster will hit your business — it's only a matter of time.

Business interruptions from natural disasters, vendor breaches, and ransomware make business continuity mission critical for businesses in order 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.

Disaster recovery tests must be conducted in an objective-driven way and are often audited as part of compliance assessments. These include:

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

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

Tabletop Exercises and Plan Walkthroughs

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

What are Your Recovery Time and Recovery Point Objectives (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 a business 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 toward recovery drills is an additional layer of strength in a compliant security plan.

Do you have all five aspects of a compliant security program?

Test your business's cybersecurity posture against the five core components of compliant security.

START

1 Are you aware of IT risks, compliance regulations, and cyberthreats facing your business today?

YES

We have already identified risks and regulations.

NO

We have not thoroughly identified the latest risks and regulations that could impact our business.

There's no one-size-fits-all to cybersecurity, and identifying the risks and requirements specific to your business is fundamental to designing a compliant security program.

2 Do you have IT governance in place for internal team members such as access control, regular training, or documented compliance regulations?

YES

Internal IT governance is in place and enforced.

NO

We trust internal teams to protect data and devices on their own.

While you may trust your teams, remember that your stakeholders will hold you and your company accountable if a bad apple turns up. Implementing internal safeguards can save your data — and your reputation.

CONTINUE

3

What approach do you use to detect potential IT threats?

A

We have an internal Security Operation Center (SOC).

Is your SOC active 24/7/365? Are they regularly trained on new tools and practices? These are questions to consider to strengthen your SOC and overall security posture.

B

We use cybersecurity tools and platforms to monitor IT environments.

Does your company have the expertise to act in case of an emergency or does it just have the tools to let you know that there is an emergency? Security tools always require the human element in order to respond, mitigate, and recover.

C

We work with an outside team for some or all cybersecurity services.

Have you vetted your third-party team? While partnering with experts can greatly improve your security posture, don't drop your due diligence when it comes to any outside resource accessing your IT systems.

D

We use a combination of internal teams, tools, and/or third-party resources.

CONTINUE

4 Do you have a crisis communication plan documented with responsibilities assigned?

YES

We have a well-documented communications plan with assignments.

NO

We have a general plan if a crisis occurs, but it is not well-documented or assigned to anyone.

A swift response can minimize reputational damage and retain trust with stakeholders, and the best way to ensure that is possible is by documenting and clearly identifying who has what responsibility in a communication plan.

5 How often do you test your disaster recovery plans?

A

We test our DR plan frequently to stay up to date and/or prepare for compliance audits.

B

We have a DR plan, but we do not test it on a regular basis.

Cyberthreats are constantly evolving, and so should your recovery plans in order to meet new risks to your business IT. Testing your DR plan not only provides better peace of mind, but it is also often a requirement for many compliance standards.

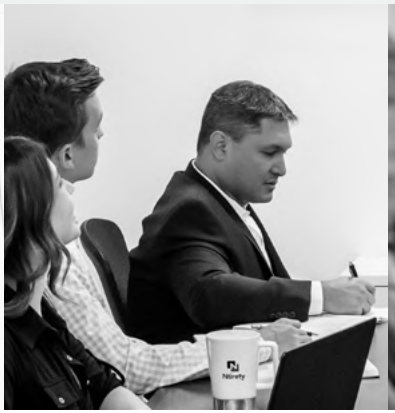
CONTINUE

Good job — but keep going!

Even if your business can successfully check off each of the five aspects of compliant security today, it doesn't end there. The business IT landscape is constantly changing, and cybercriminals always aim to be one step ahead of the curve. The best cybersecurity plan is one that grows and adjusts with your business, industry, IT environments, and risks.

About Ntirety

With over two decades of successfully operating, managing, and securing private, public, and hybrid cloud environments, Ntirety has led enterprises across industries through the volatile early days of data hosting into the world of 24/7 managed security with our premier Compliant Security solutions. Through cost-effective and scalable solutions tailored to business-specific needs, Ntirety eliminates gaps in both security posture and compliance documentation by delivering solutions that cover the entire application and the entire compliance and security process, the entire time.

SOURCES

1. IMB Cost of a Data Breach Report, 2020
2. 2019 Data Breach Investigations Report
3. The State of Ransomware in the US: Report and Statistics 2019
4. 2020 WFH Employee Cybersecurity Threat Index
5. Ponemon Institute 2019
6. BlackHat Hacker Survey Report 2017
7. Bitglass 2020 BYOD Report
8. 2017 Email Security Report
9. Cybersecurity Market Report 2019
10. Infosec Institute 2019
11. 451 Research: Voices of the Enterprise – Information Security Businessal Dynamics | Q2 2019
12. Forbes 2019: As The End of 2020 Approaches, The Cybersecurity Talent Drought Gets Worse

Ntirety

WWW.NTIRETY.COM