Secureworks®

WHITE PAPER

# Cybersecurity Policy 101: Avoiding Gaps and Staying Secure

The importance of establishing a robust cybersecurity policy

Data breaches and cyberattacks today are not a matter of “if,” but “when.” Each employee represents a potential vulnerability who – if not properly trained – may unwittingly welcome cybercriminals through the organization’s backdoor. As a result, business leaders should take the time to establish an official cybersecurity policy that will underscore the importance of security to the business and empower employees to do their part in protecting sensitive data and IT systems.

**No matter the size of the organization, every control has a cost. With that in mind, it’s critical that each policy makes good business sense—if the cost of the control is greater than the risk to the business, that policy should be evaluated based on potential financial, reputational, or compliance risk to the business.**

## The Main Elements of a Strong Cybersecurity Policy

A cybersecurity policy should serve as an organization’s bible, setting clear guidelines on behavior from how data should be stored and transmitted, to which activities are restricted. Good policies cover both expectations, which will be followed by all users on the network, as well as internal responsibilities, which will be primarily administered by the organization’s security leaders. These policies should be written to apply not only to employees, but also a company’s vendors, contractors, and guests – essentially, everyone that could potentially put the organization at risk. User-facing policies may include directions and mandates for items such as how to handle a suspicious email, or how to build a strong password. In contrast, administrator-facing policies generally focus on how the organization will manage and operationalize the services providing security. It may be helpful to delay the User policy until the Administrator policy is in place, since it generally informs the former from the type of network security to the levels of access management and control.

Depending on the size of the organization, there are two common ways to organize policies. Typically, large organizations create a policy for each service area, such as access control, malware anti-virus, and vulnerability management. For smaller organizations with a staff that supports multiple services, one information security policy may cover all the areas.

## Common Mistakes in Establishing a Security Policy

Without a strong security policy, organizations can open themselves up to unnecessary risk and uncertainty. The mistakes organizations frequently make include:

**Lack of employee accountability:** It’s not enough to have a policy; users need to be aware and trained on how to follow it. Policies should be built into learning management systems and shared with employees upon hiring with reminders sent in regular intervals. The consequences should also be clearly stated, with any employee that doesn’t follow the guidelines disciplined, or vendors with contracts terminated, etc.

**Outdated policies:** Policies should also be reviewed at least once a year to ensure they are still relevant. For example, does your policy cover the newest tools and social media platforms? Has the business environment changed significantly? Following the impact of COVID-19, additional provisions may need to be made to address policies covering remote work and the use of personal devices for work functions.

**Overly focused on reactive measures:** Some organizations may make the mistake of only focusing on reactive measures in the event of a security incident. Remember, the best defense is a good offense. In addition to training employees on what to do if they're the victim of a phishing or ransomware scam, your policies should also cover expectations concerning proactive security measures. For example, how often to run a security scan on your machine and guidelines around accessing sensitive work data on personal devices.

**Not incorporating cybersecurity into business continuity plans:** Business continuity plans have traditionally focused on how organizations can recover following a physical disaster, such as a fire, flood, or hurricane. Due to the reliance on a mobile workforce, there may be a tendency to make these plans leaner, but while traditional disasters may no longer pose as big a threat, the climate today is even more favorable to would-be cybercriminals. In response, leaders should seek the input of their IT departments on their business continuity plans, to advise and help on the front lines following a cybersecurity incident.

## Potential Risks of Gaps

Having an official cybersecurity policy may not seem like a top priority for a business focused on the daily running of its operations, but the consequences can be myriad. Similar to washing hands, practicing basic cyber hygiene should be a critical part of any organization. Employees working from home need to be reminded to be vigilant about their security in order to avoid putting their organization at greater risk. This should include updates about the latest security risks, which are constantly evolving.

Users need a clear understanding of penalties. Employees may be more likely to engage in negligent behavior, particularly given increasingly blurred lines between work and home. For example, the temptation may be greater today for employees to use an unsecured network or personal laptop for work, as well as to post about their latest projects on social media websites.

In addition, COVID-19 illuminated the potential pitfalls of not having a strong business continuity plan in place to protect the organization against security risks. Many businesses are already struggling to adapt to the changes the pandemic has brought and can't afford to deal with yet another unplanned issue. If an organization were to discover a data breach at this time, their business continuity plan would be essential for aligning IT teams and leadership on next steps and how to best protect customers and employees as they move forward.

## The Need for Executive Sponsorship

Potential risks should be clearly communicated to senior leadership in order to generate full buy-in. Creating a robust security policy framework requires the efforts of a cross-company information security committee, which should include representation at a high level – for example, the CEO, general counsel, HR, and business unit leaders. This ensures that the IT department is receiving the resources and support that they need to be successful. The committee can also help integrate security consistently across the business, from the HR official handbook to the legal agreements with vendors.

CEO involvement is essential for underscoring the importance of following security guidelines. Knowing that the CEO supports the security measures and consequences for negligence can be a strong motivator in encouraging compliant behavior. Aligning the different business functions around a central policy also helps to reinforce the role security plays across an organization and eliminate confusion.

Once senior leadership has come to support the policies, an external assessment is a great way to identify any additional gaps. An outside vendor can help pinpoint and prioritize areas that need to be addressed or are not robust enough. In addition to the fresh perspective that an outside party can bring, an external assessment can lower organizations' risk ratings in a number of ways. First, overall employee management, by decreasing the ability for an employee to point to an outdated clause and claim they "didn't know" about the policy.

**An assessment can also help sell the need for stronger measures to business units that might not see how they're directly affected. For example, marketing may not be thrilled with stricter guidelines concerning their use of online websites and social media but outlining the impact that a data breach could have on their brand may help them understand.**

## Strengthening Your Organization for the Future

Ultimately, working to identify and address the gaps in your company's policies will strengthen your overall security posture, both now and in the future. Developing a robust policy, reinforcing it through regular training and reminders, and through consistent review and consultation with the information security committee and senior management, can ensure security stays top of mind for your organization. If recent times have taught us anything, it's that preparing for an unknown future is the best way for an organization to not only survive but thrive on what's to come.

Secureworks®

## Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

## Corporate Headquarters

**United States**
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

## Europe & Middle East

**France**
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

**Germany**
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

**United Kingdom**
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

**United Arab Emirates**
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

## Asia Pacific

**Australia**
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

**Japan**
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp