Cybersecurity During Uncertain Times

BARR ADVISORY

Table of Contents

Introduction

Over the past few years, the world has faced unprecedented circumstances that have heightened overall security risks. In fact, the search term “cybersecurity” recently hit an all-time high. This search trend says a lot about the current moment. Cybersecurity can be hard to understand and means different things to different people—it encompasses various domains and grows year over year. Between global tensions, political turmoil, and the pandemic, there’s a fear factor that comes in with the unknown of cybersecurity. When people start to hear the term in the news, they want to figure out what it means and how it impacts them.

With the rise in cyberattacks increasing every year, it’s critical to understand the multiplicative nature of cybersecurity risks with global challenges. This whitepaper will explain how to prioritize security by getting back to the basics and how to build a human-first business continuity plan.

Cybersecurity: Back to the Basics

From big data breaches in the headlines to dark imagery of hackers in hoodies, there are unfortunately a lot of scare tactics in the cybersecurity industry. This can make cybersecurity seem intimidating to even the most well-equipped organizations, especially those that feel they need to be doing everything at once. But if you know where to start, focusing on implementing the basics and doing them well can help your organization navigate through uncertain times.

Let's take a look at a few examples of cybersecurity fundamentals every organization should have in place.

Asset and Data Management

You can't protect your data and assets if you don't know where they are. It's also important to understand what types of data you have to determine if there are any regulations that may apply to your organization's security. You should also know who owns and maintains any information assets and how important those assets are to your organization.

Multi-factor Authentication

Multi-factor authentication (MFA) prevents hackers from breaching your accounts by requiring a password AND a one-time code sent to another device. Accounts with MFA enabled have been proven to be more secure than accounts without it.

Credential Management

Vulnerable user access has been the cause of a number of high-profile data breaches. Credential management involves managing the lifecycle of all credentials in the organization used for authentication, from creation to access updates, revocation, and replacement.

Patch Management

Patch management is the process of updating software in order to correct errors or vulnerabilities. Staying on top of patch management is critical to reducing the likelihood of a vulnerability being exploited.

Thoughtful Risk Assessments and Threat Modeling

Even asking the basic questions around risk assessments can help your organization understand what it needs to protect. Questions such as “what percentage of accounts do not have MFA?” and “What percentage of systems are exposed to the internet?” can help determine the risks posed to your specific organization.

Threat modeling is the process of identifying potential threats (such as vulnerabilities), communicating them, understanding them, and mitigating them.

Cybersecurity experts have been advocating for these basic practices for years because they work. Time after time, these fundamentals are shown to help mitigate cybersecurity risks for organizations of all sizes. By implementing these simple cybersecurity measures and focusing more on what can go right with these practices in place instead of what might go wrong, it can help break through some of the scare tactics surrounding cybersecurity.

If you already have the basics implemented, many of these practices are easily scalable as your organization grows. The threat landscape is constantly evolving, which means it’s not enough to implement the basics and stop there. Responding to new threats as they arise in real time and staying on top of cybersecurity trends is a key aspect of building cybersecurity resilience.

How to Anticipate Top Threats

There are a number of frameworks and resources available that can help your organization anticipate top threats. These frameworks can serve as a great checklist to help your organization check itself internally.

Let’s take a look at two frameworks that are useful for anticipating threats:

National Institute of Standards and Technology (NIST)

NIST 800-53 is a catalog of security and privacy controls designed to protect against security issues. It can be helpful to go through each one to reduce your organization’s risk, as the controls cover everything from technology to management and training practices. There’s also a lighter model, NIST CSF, that contains more of the detailed security controls from NIST 800-53, which can make it easier to approach cybersecurity.

Center for Internet Security (CIS)

The CIS controls are a prioritized set of actions to protect organizations and data from cyberattacks. CIS has both a top level framework as well as very specific benchmarks for the systems your organization might have, whether it’s a different cloud or Linux systems. These benchmarks can help harden and secure those systems.

How to Anticipate Top Threats

The Cybersecurity and Infrastructure Security Agency (CISA) website is an excellent resource for organizations when preparing for the increased risk of cyberthreats. As a government agency, they stay on top of threats to U.S. companies and provide free cybersecurity tools and services. They also have cybersecurity action plans for organizations of various sizes that provide insightful guidance on how to create a cybersecurity program.

It can also be helpful to review a few well-respected industry reports like the annual Verizon Data Breach Investigations Report as they are released each year. These reports are essentially free threat intelligence—they can tell you what the most common threats and cybersecurity risks out there are, how they happen, and how to prevent them.

Given the number of frameworks out there, it’s better to adhere to one of them and do it well rather than overwhelming your organization by trying to do everything all at once. It’s also important to keep in mind that while these frameworks are very useful, they may not be updated regularly with every new threat out there. That’s why it’s also important to plug into the cybersecurity and business communities, such as your local tech council, to participate in conversations around security trends and help build your own expertise.

Establishing a Business Continuity Plan

Every organization needs a business continuity plan—a plan that outlines how your organizational operations will continue to run in the event of disruptions. These plans may look different for each organization depending on their unique operations, but the essential focus of every business continuity plan is people, processes, and technology. A strong business continuity plan will address how to keep each of these factors safe and functioning in the event of an incident. For each factor, organizations should focus on increasing resilience, establishing a recovery strategy, and making a contingency plan.

Between the pandemic, war zones, ransomware, and natural disasters, the world has certainly been facing challenges in the past few years. While it's easy to panic during uncertain times, these difficult times can be used as an opportunity to create a budget and obtain the necessary resources for contingency planning. These real-world scenarios can help begin your business continuity plan by focusing on how people, processes, and technology are affected in each scenario. There are plenty of templates available to help you build your business continuity plan, but these scenarios allow you to walk through each potential issue that your business could face and learn from it.

Lastly, when you have a problem or issue arise, turn it into a project. Not only does it make it easier to forget the worry the issue is causing, it becomes an action item that is ready to be solved. While it can be difficult to plan for worst-case scenarios, establishing a strong business continuity plan builds resilience.

A Human-First Approach to Business Continuity

For a lot of organizations, it can be easy to think through the processes and technology aspects of their business continuity plan. If you need a new app or tool, there's likely a number of products available for you to demo and purchase that can suit your needs. If someone in your organization broke their laptop, you can order a new one online and have it delivered the same day.

It can get trickier with the people aspect. Technology isn't much use to your organization if there's no one to use it. So much internal knowledge is built up within each team, their shared experiences, and how they do their job each day—so if someone critical becomes unavailable due to sickness, how do you manage it? There has to be a plan for who can step in and take over until they recover, and just as importantly, a plan for supporting the person when they can come back to work. All of these steps are important to contingency planning in case someone is temporarily or permanently unavailable.

Let your culture and core values guide you. When an issue arises, use it as an opportunity to align with your mission. When you take a human-first approach to business continuity, it's not a transaction—it's about prioritizing the well-being of the people in your organization first and foremost.

About BARR Advisory

At BARR Advisory, we build trust through cyber resiliency. We help protect the world's data, people, and information networks through a human-first approach to cybersecurity and compliance. Businesses looking for the accessibility of a boutique firm with the tools and expertise of a global consulting firm will find a partner in us.

Specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud, BARR has the global network of partners, the perspective, and deep expertise every thriving SaaS provider to world-class enterprise needs to stay secure and compliant at every stage.

Our Services

SOC Examinations
[SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]

Healthcare Services
[HIPAA/ HITRUST]

ISO 27001 Assessments

FedRAMP Security Assessments

PCI DSS Assessment Services

Penetration Testing and Vulnerability Assessments

Virtual CISO Services

People & Culture Services

Connect with BARR

Want to learn more about the role of the CISO or if your organization could benefit from a virtual CISO? Contact us today.