SpiderOak

White Paper | 2018

Five New Rules for Keeping Your Company's Data Safe

Jonathan Moore
Chief Technology Officer
jmoore@spideroak-inc.com
+1 866.432.9888 x702

Matthew Erickson
Dir. of Client Services and Technologies
matt@spideroak-inc.com
+1 866.432.9888 x703

SpiderOak, Inc.
4741 Central St #324, Kansas City, MO 64112
info@spideroak-inc.com
+1 866.432.9888

2018 is the year you can secure your data against cyberattacks. But it takes a fundamental shift in thinking to do it.

New enemies at the gate

As recently as 5-10 years ago, nearly any solid product a company purchased to secure its data and systems looked like it worked. There were small incidents, but there seemed to be little indication of truly massive, company-destroying breaches. Today, we see one major headline after another – from the devastating breach at Equifax to Yahoo's record-breaking 3 billion user accounts compromised – even after companies have added significant encryption upgrades. What has changed?

A key difference lies with who the bad actors are today – a very different set of adversaries than those who threatened data security in the past. The adversaries today are much more advanced and much more persistent in their efforts to steal from you or learn from you. From criminals hacking personal and financial data, to ransomware, to nation-state actors conducting espionage and sabotage, hackers have shifted from largely sole perpetrators to much more organized, well-funded, and complex crime rings, botnets, and national intelligence agencies who find a thriving market for stolen data on the Dark Web. The entire landscape of cybercrime has changed.

What's driving companies to spend nearly $100 billion annually on cybersecurity?

- **An average breach costs $3.5 million**
- **In 2016 alone, SMBs paid $301 million to ransomware operators**

The failings of the "castle" model of data security

The modern adversarial environment has advanced so rapidly that current approaches to mitigating risk are having their impact severely limited or completely curtailed. You can't just build higher walls and deeper moats around your centralized server – the whole fortified "castle" model of protection leads to inevitable compromise.

At this point, nearly all companies have been convinced that they must act around cybersecurity – the fear is out there, and they are throwing money toward products aiming to keep their systems safe. The problem is that spending doesn't constitute a real plan. Higher walls around your data will just lead criminals to build taller ladders, and once one door is breached, the entire complex falls.

Attacks are inevitable, but massive, costly breaches are not.

With the pace and scale of attacks, and their associated costs, growing at a more rapid rate than ever before, companies have adopted a resignation about the situation. Despite all the sophisticated systems being put in place, are massive breaches inevitable?

At SpiderOak, we believe not. In fact, it is possible for a company to vastly reduce the damage and scope of attacks, even in the midst of unprecedented new techniques from attackers. Budget that today has to be spent on costly cyberinsurance premiums and breach clean-up can be spent on producing real value for the business. Attacks may be inevitable – and threaten every single business on the planet – but massive, costly breaches are not.

A foundational shift in what it takes to keep your company healthy

In order for companies to successfully keep their business and balance sheet healthy for what will become an even greater threat in the months and years ahead, there must be a complete shift in thinking about data and systems security. This foundational shift in approach to cybersecurity relies on five core elements that company leadership must adopt in the new reality of cyberattacks.

We identify below the critical steps to ensuring that your data and software are protected and that any potential damage is significantly constrained.
By embracing these steps and driving these actions and behaviors down into the organization, CEOs and their executive teams, as well as the board of directors, can turn what could have been a multi-billion-dollar problem into one that barely affects the balance sheet.

5 new rules for keeping your company’s data safe

Rule #1: Have a clear inventory of what data is critical to your organization.

If you suffered a breach today, what would cause you to be out of business tomorrow? Most organizations lack a clear understanding of what data and data flows exist within their systems, making it impossible to know what to secure, and if breached, what the impact actually is.

The first piece in being able to secure data is conducting an audit of what data you have – who produces it, who consumes it, what processing is done to it, and which pieces are mission-critical to your organization. The era of Big Data has driven companies to collect as much information from customers as possible, whether or not they even have at the time the tools in place to leverage that data. This amassing of data presents opportunities for greater monetization, but it also presents greater risk. Vast pools of financial and personal information are sitting in your organization, and you may not even be using it. Data is a liability that can be measured in dollars, and most companies hoard it without a second thought.

In creating an inventory of all the data retained and its purpose, a company can then identify which pieces are necessary to its ongoing operations and which are not. While the ideal is to be able to have all your data secure, the reality is that this cannot happen overnight. Companies need to be able to triage – to invest immediately in the high-value and easiest-to-protect data. With a data audit, prioritization, and triage, company data security can focus on what needs to happen first and allocate resources accordingly.

Rule #2: Create a "two-person rule" for your data and processes.

In every movie set in a Cold War submarine, there are two stern-faced naval officers looking at each other as they both turn the keys to fire missiles. Each officer has his own responsibilities in validating and carrying out orders, and, when they agree – IF they agree – they both turn the keys. Likewise, in your accounting department, you probably already have dual-signature checks and other oversight measures on your cash flow. Most companies, however, lack the same level of accountability across the rest of the organization. And we have seen with the false missile alert in Hawaii that even the civil defense can allow one person to drive a single monumental error.

The common approach to securing data today implicitly trusts many people within your systems with varying amounts of independent authority. Likewise, the common approach to preventing abuse or misuse of authority amounts to monitoring in order to track issues as they happen at best, or commonly, simply providing forensic analysis after the damage is already done.

By making sure critical operations and data access are guarded through multiple authorities, each checking the validity and work of the other, you minimize the risk that a compromise of any one part or person in the system compromises everything.

Rule #3: Compartmentalize your data.

Millennial employees aren't the only ones guilty of oversharing. Corporate America has made this a standard practice for decades: over 70% of employees have access to data they don't need to do their jobs (Ponemon Institute).

Companies keep multiple layers of data related to its operations – from financials and customer information to the organization's intellectual property, employee SSNs, and company emails. In the vast majority of cases, this data is concentrated in one or just a few servers, where the data for one purpose is connected to data for another. This creates a network of linked exposure; a breach in one area can domino quickly into a breach of another database.

Thus, if the CFO gets specifically targeted and compromised, it is not only his financial data that is compromised; the hacker can the access whatever is linked to the data, including highly confidential customer information. If a customer support system gets compromised, your CEO's communications with the board may be at risk.

By making sure that the ability to view and work with data in an organization is aligned with job responsibilities and enforced technologically, you can make sure that any one failure of security is not a total failure of security for the organization.

Rule #4: Build your defense in depth.

Any company that's on the Internet does not have a perfectly closed-off network connection. Your website, any services you offer, your corporate email, and more have to face the public Internet, and, therefore, are holes in your security. There are always going to be bugs, in- or outside of your control, that let attackers take control of any public-facing services and servers.

Unfortunately, most companies don't have effective defenses internally between systems. In the interest of cheap and easy deployment, combined with fearing performance penalties among internal systems, most organizations have wide-open security configurations. In this world, it only takes one breach for attackers to leverage unsecured internal systems to gain access to their target.

All of this could be stopped by simply applying the same security principles a company applies to its public-facing servers to its internal systems as well: setting up firewalls, using encrypted communication, and requiring strong authentication methods.

Ultimately, the need for security – not the need for performance – must drive the conversations around data controls. For many companies, this is a hard pill to swallow. But the cost of bypassing these controls, in the form of a breach event, will exponentially outweigh the marginal gains in giving away too much access.

Rule #5: Keep the keys to your kingdom offline.

Modern security relies on minimizing the number of things you have to trust. If you are not encrypting your data, compartmentalizing it, and understanding to whom you are granting access, you are effectively creating an infinite number of things you have to trust to be secure. It's likely that a failure in one vendor's vendor down the line can result in real vulnerabilities for you. By employing the four rules above, companies will have a very limited number of things to have to trust: the secrets involved in decrypting your data. For there to be a complete and massive compromise of your business, a cybercriminal has to find and obtain those secrets.

Today's computing environment, from the CPU up to the web browser, contains millions of ways to enable attackers to compromise systems and get those secrets. But organizations can use hardware tools today that, based on cryptography, enable them to keep their closest secrets on special USB keys. When not in use and connected to a system, those devices can be kept in a safe. Thus, even if attackers get complete control over an organization's computers, if the secrets are stored and secured in this way, it would be impossible to expose sensitive data.

Conclusion: Going Forward

Getting an organization’s data and systems setup to support a healthy company demands some tough choices. But as companies start to see enormous losses from breaches in the form of disrupted business, damaged reputations, embarrassing revelations, remediation costs, and more, CEOs and executive teams are going to be under increasing pressure to rethink how their organizations are protecting themselves against attacks. It is only by adopting these new “rules” of cybersecurity that companies can be playing the same game as hackers today, and actually get out in front of the challenge.

About SpiderOak

SpiderOak provides mission-critical data and systems security for organizations and individuals. Using the latest and most secure blockchain technology and encryption, paired with identity management, SpiderOak’s platform defends client assets, intellectual property, and operations against military-grade cyberattacks. Our offerings include an enterprise platform protecting all of an organization’s data, software, applications, and devices; a secure software updater allowing companies to develop and update their applications in a secure way; and secure backup, messaging, file sharing, and storage for large and small businesses and individuals. For more information, please visit https://spideroak.com.

More information

To learn more about how your company can protect its data and become more secure, please contact us.

Christopher Skinner

CEO
cskinner@spideroak-inc.com
+1 504.259.6700

Jonathan Moore

Chief Technology Officer
jmoore@spideroak-inc.com
+1 866.432.9888 x702

Matthew Erickson

Director of Client Services and Technologies
matt@spideroak-inc.com
+1 866.432.9888 x703