Nine Surefire Steps to Lock Down Your Cybersecurity

Your organization depends on the trust you develop with your stakeholders. That means following nine key cybersecurity steps.

By Clinton Henry

There's no good way to tell someone that their data's been stolen. While a security breach might be one of the last things on your mind, the most recent Travelers Risk Index report shows that it's a top concern for your clients and customers: "Personal privacy loss and identity theft" went from barely ranking on their survey a few years ago to being #2, right behind "financial security."

You need to address cybersecurity with the same fervor that you meet all the other expectations of your stakeholders. To do so, follow these nine steps:

1. Engage and educate your employees

It's important to create a culture of security within your organization, because security is everyone's responsibility. If you don't have buy-in from all your team members, you're exposing your organization to unnecessary risk. Most attackers gain access to networks by manipulating someone within an organization, not via hacking from a dark, Cheetos-filled basement somewhere, as the movies often portray. Why would someone spend days trying to crack your accountant's password when they can simply call, pretending to be your accountant, and ask a staff member to reset the password to something new?

> "Did we just guess your password? Go change it!"

2. Use anti-virus software on every desk

Having up-to-date anti-virus on *all* desktops and servers is vital. An unprotected computer is an easy target for a motivated attacker. Pay for anti-virus software, and make sure it's regularly updated.

3. Manage passwords

It's essential that you and your employees leverage strong, complicated passwords that aren't easy to guess. Attackers now use hacking applications that run through the most common 10,000 passwords in about four minutes, trying

> “Most attackers gain access by manipulating someone within an organization.”

each of them. You’d be surprised how many folks with access to critical data have the password of “password” or, if they’re feeling clever, “password1.” (Did we just guess your password? Go change it!).

4. Guard your networks

Having a firewall between your organization’s networks and the internet is crucial. If you don’t, there’s very little stopping someone from freely accessing your data.

5. Secure the cloud

No matter what cloud provider or service you use, do your due diligence on their security practices. If they can’t easily and quickly tell you how your information is secured, odds are it isn’t. For any accounts used to access your organization’s data, make sure you have strong passwords. Access those accounts only via a computer you own or trust. If you access your cloud on an infected machine, a hacker could learn your password and use it later without your knowledge.

6. Protect your banking information

Be certain that all financial data, accounts, and records are kept secure and segregated from the rest of your organization’s general shared drives. If financial transactions are conducted electronically, ensure that’s done over an encrypted connection and that your employees never e-mail account numbers, credit card information, or sensitive financial documents.

7. Back up your data

One of the most common breaches now being seen are ransomware attacks. Instead of “stealing” data from your organization, these attackers find your critical data and then encrypt it (digitally locking you out of it), so that only the person with the digital “key” can unlock and access that information. The hackers then offer the victim access to the “key” for a very large fee. If you’re hit with one of these attacks, you have two options: Pay the fee, or restore the locked data from a recent backup. This is why backups are so important. Recently a hospital, a police department, and a public school (along with literally thousands of other victims) were forced to pay tens of thousands of dollars to get their data back. Making sure your information is backed and stored separately from your main repository can help protect you from attacks such as these.

Don’t Take Risks with Your Precious Data

For more, see these articles at NonprofitWorld.org:

Workplace Identity Theft: Curing the Latest HR Headache (Vol. 25, No. 5)

Cybersecurity: Not Just for Home Depot Anymore (Vol. 34, No. 4)

Don’t Get Caught by Phishing Schemes (Vol. 35, No. 2)

The Cloud: Software Transformation & Evolution of the Workforce (Vol. 33, No. 1)

Create a Powerful Culture (Vol. 35, No. 2)

Avoid Catastrophe by Addressing Cyber Risk (Vol. 33, No. 3)

Wire Transfer Fraud: It Could Happen to You (Vol. 35, No. 3)

Keep Your Online Identity Safe (Vol. 35, No. 4)

Mitigate Cyber Risks with the Right Security Controls (Vol. 36, No. 1)

8. Protect physical documents

You’d be surprised how much sensitive information is left lying around the office. Ensure that your partners, trusted employees, and finance team lock away any such documents when they aren’t working with them.

9. Secure everyone’s mobile devices

While they’re a convenience, mobile devices mean that sensitive data can walk out your organization’s door without you ever knowing it. Make sure that all mobile devices used to access organizational data have passwords (your e-mail server can force this requirement). If you have employees who use laptops, look at having the hard drives for those machines encrypted. Most modern operating systems have encryption built in; you just have to enable the feature, and it’s foolish not to leverage it. If an employee accidently leaves a laptop on a plane or in the back of a taxi, you’ll be guaranteed that everything on it is secure and protected.

Clinton Henry (clintonhenry.com) is one of the world’s leading cybersecurity and identify theft experts. Known for his engaging keynotes and insightful perspective, Clinton has amassed a loyal following of executives who look to him for guidance on how to protect their organizations’ reputation from attack or compromise.

> “There’s no good way to tell someone that their data’s been stolen.”