What to Do When an Employee Becomes a Cybercriminal

Your greatest security threat may come from inside your organization. Use these tactics to protect your data.

By Bryce Austin

Today's cybercriminals come at your organization from many angles. They're organized. They share information amongst each other. They're often well-funded. They're more dangerous than ever before. And they may be among your employees.

Employees may breach your sensitive data to sell it or as an act of revenge if they feel underpaid, underappreciated, or unhappy with your organization in any way. If you fall victim of a malicious-intentioned employee, finding out what happened is difficult because such employees often have system privileges that allow them to erase their tracks.

While it's true that internal employees are responsible for a large number of cybersecurity breaches, it's also true that most of these are unintentional. Most breaches are a result of good people doing something they shouldn't, either out of ignorance or because a cybercriminal tricked them into doing it.

Statistics on the exact percentage of "insider" cyber breaches that are deliberate vs. inadvertent vary widely, but most experts agree that the vast majority of insider threats aren't malicious. No matter which statistic you believe, everyone agrees that many threats would have been prevented if the insider had understood how his or her behavior allowed a breach to occur. The keys to mitigate these risks are simple:

Educate your employees.

Establish a cybersecurity training program for your employees. Hold this training frequently, and make it mandatory. Clearly lay out the policy for cybersecurity and the consequences of violating the policy.

Don't let employees take home devices that contain sensitive files. There's always the risk of the device being stolen or sensitive data being transmitted over insecure networks at their home or other locations.

Instruct your employees never to share their passwords.

Know your people.

Perform background checks on your employees to identify those who might take deliberate actions that would harm your organization.

Know which people have access to the most sensitive data.

Guard your most sensitive data.

Limit your employees' ability to obtain access (intentional or unintentional) to sensitive information via a least-privileged approach to your data.

Identify your most sensitive and valuable data. Then assign that information the highest safeguarding and most persistent monitoring.

Remove "local administrator privileges" from your users to their laptops or desktops. "Local administrators" are those who can do anything they choose with a computer, such as install programs, delete files, change sensitive security settings, and so on.

Turn on "egress filtering" on your network, and limit the use of USB thumb drives. Those precautions will make it harder for anyone to make copies of information and move it out of your organization.

> "Limit the use of USB thumb drives."

> "Your employees can be your greatest liability."

Ensure that you have forensics available to you.

Tracking down an internal cybercriminal requires logging of network activity, especially for any access to sensitive information.

Any logs need to be stored in an area that is limited to the fewest number of employees as possible.

Yes, your employees are your most valuable asset, but they can also be your greatest liability. They need to be trained on best practices to keep your data safe, and they also need to understand that you have forensic systems in place that will likely catch them if they attempt to access data they shouldn't.

Bryce Austin (bryceaustin.com) is the CEO of TCE Strategy, an internationally-recognized speaker on emerging technology and cybersecurity issues, and author of Secure Enough?

Trust But Verify

A "trust but verify" approach regarding employee access to your critical intellectual property is an important part of your cybersecurity program. For more strategies in keeping your data safe, see these articles at NonprofitWorld.org:

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

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

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

Use Background Checks to Avoid Legal Pitfalls (Vol. 29, No. 1)

Hacking People: Why Your Biggest Vulnerability Isn't in Your IT Department (Vol. 37, No. 1)

Are You Prepared for a Cybersecurity Incident? (Vol. 38, No. 4)

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

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

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

Nine Surefire Steps to Lock Down Your Cybersecurity (Vol. 36, No.3)

please get in touch...

We would love to hear your response to anything in **Nonprofit World**, your comments about any aspect of the nonprofit sector, and your concerns about your daily work. Please get in touch in any of the following ways:

Drop us a note at: Letters to the Editor, Nonprofit World, P.O. Box 44173, Madison, Wisconsin 53744-4173.

E-mail to: muehrcke@charter.net

Please include your name, organization, address, phone number, and e-mail address. If you'd like your comments to appear anonymously, please let us know. We look forward to hearing from you!

WHAT'S UP ONLINE?

Would you like to discuss some of the issues addressed in ***Nonprofit World*** with other nonprofit professionals? Do you have questions to ask or expertise of your own to share?

Society for Nonprofits is actively engaged on LinkedIn, Facebook and Twitter. Find us on your favorite social media platform by visiting **social.snpo.org**

If you have any questions, contact Jason Chmura at jchmura@NonprofitWorld.org