DecisionHealth

My Account | Log Out | About Us | Help |

Part B News COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES

Advanced Search ◀

Home | News & Analysis | Regulations & Guidance | Communities | Training & Events | CEUs | Store |

Home | 10/14/2021 Issue | Article

Inside job: Use tech, common sense to repel employee threats to your cybersecurity

by: Roy Edroso

Effective Oct 14, 2021

Published Oct 18, 2021
Last Reviewed Oct 14, 2021

Cybersecurity

Recent headlines about a practice employee who absconded with her boss' password serves as a reminder that the biggest threat to your cybersecurity could be right under your own roof. Set some clear boundaries for your employees' network access and be prepared to decommission them swiftly when it's time to cut them loose.
In the cybersecurity case, police in Alexandria, Va., were trying to track down a former practice employee who'd left her physician employer on bad terms because "the recovery account for his email belonged to the former employee," according to reports. The missing woman has been threatened, though not charged, with "computer trespass" under Virginia law, a Class 1 misdemeanor.

Look around and you'll find many cases of medical employees who've gone rogue and caused more far-reaching problems for their employers. Unity Health Hospital in Toronto, for example, reported in October 2020 that a medical transcriptionist formerly employed there "had taken and kept copies of several reports that he had transcribed" and used these files to try and extort money out of them, according to a report.

Insider incidents

When you consider the damage employees can do to practice cybersecurity, you probably think of them thoughtlessly clicking a phishing link and unleashing a ransomware attack (*PBN 4/26/21*). But it may be more likely that an employee will cause computer-enabled mayhem on purpose than by accident: A recent IBM X-Force report finds that "insider incidents made up 13% of all OT [operational technology]-related incidents in 2020, with about 60% of those involving malicious insiders and about 40% involving negligence."

"We've seen cases like this all the time on both sides," says Shari Claire Lewis, a partner in the privacy, data & cyber law practice at the Rivkin Radler law firm in Uniondale, N.Y. "The disgruntled ex-employee who in the old days would stand at the photocopy machine after hours and [copy] the client list. They don't have to stand at the photocopy machine anymore if management doesn't act quickly to lock down their access."

And it isn't always for personal gain. Sometimes disgruntled employees "just want to do as much damage as possible on the way out the door," Lewis says. "We've seen situations where they've locked down the company laptop or left Trojan Horses that, after a time, would go off and destroy data."

Arm your tech with protections

As you might expect, there are ways to assess how your employees are using or abusing your technology that are themselves technological.

Some internal security strategies use "behavioral analytics technology" and make decisions based on employee behavior they're tracking, says Steve Moore, vice president and chief security strategist at Exabeam in Foster City, Calif. Such systems are trained to distinguish between normal employee behavior and unusual activities "that are typical signs of insider threats, such as large data uploads, credential abuse or unusual access patterns," Moore explains.

"When irregular behavior is detected, it should be taken seriously as a possible attack," Moore says. "Various indicators of insider threats exist, and a crucial step in protecting against them is recognizing those signs and establishing a threshold of normal [behavior] for employees."

Alternately, you might employ a strict Zero Trust security strategy. This is not based on an analysis of employee behavior after the fact, explains Julie Preiss, chief marketing officer with Appgate in Miami, Fla. Rather, it is a system that doles out access based on "pre-determined policies you 'program' into the solution." The employee's clearance is limited and continuously evaluated to see whether it needs to change based on new factors, such as roles the employee has taken on or abandoned in the organization.

"Trust is not implied simply because you're a known user like an employee," Preiss says. "Access is explicit, conditional and continuously monitored for change."

For example, "an employee of a health care company who works in sales should likely never have access to patient heath information records," Preiss explains. An IT worker may be given access to a Help Desk system in order to fix a problem,

HI ROY ☆ My bookmarks

Current Issue
Click here to read latest issue.

QUICK LINKS

click icon to expand

but once that ticket is closed, access is automatically withdrawn. “If the employee went rogue, the amount of damage they could do is limited,” Preiss says.

In such a system, when an employee is terminated, all their access can be removed at one quick stroke.

A further data protection step compatible with Zero Trust is tokenization, the practice of portraying information in the system as a token — that is, as meaningless text that appears in the place of sensitive data when unauthorized users access it.

According to Alex Pezold, CEO of TokenEx in Edmond, Okla., a familiar example of tokenization is seen in banking, where financial data is disguised in the system so that the multiple parties involved in a transaction cannot see it.

“When you process a payment using a token stored in your systems, only the original credit card tokenization system can swap the token with the corresponding primary account number, or PAN, and send it to the payment processor for authorization,” Pezold says. ”Your systems never record, transmit, or store the PAN — only the token.”

Two sets of eyes

If this seems a little extreme for your purposes, some simpler precautions based on pre-technological security models might do.

You may want to lean on “a security principle called separation of duties,” says Mark Kirstein, vice president, customer success at Cosant Cyber Security in Tempe, Ariz. “All that means is, when you’re looking at how your team’s activities and access are provisioned and how they’re going to operate on a regular basis, you want to have a very deliberate separation so that there’s more than one person involved in various aspects of the job.”

The principle is seen in corporate and financial activities that require two pairs of eyes to ensure process integrity, such as a corporate accountant who might be required to report to someone besides his boss, Kirstein says. Similarly, if you’re giving an employee elevated administrative rights to a database, requiring that two people be involved in the job “makes the execution of anything nefarious or improper much more risky for any one person to try — because they know that, in order to do this, they need the other person’s consent,” Kirstein adds.

In fact, the second party doesn’t even need to be heavily involved in the assignment — just so long as they’re present so each of the parties can vouch for the other.

3 more internal-threat thwarters

- **Use shared drives with segregated folders**. Data hostage situations rely on a bad actor’s access to other people’s work. But simply having a shared work drive with separate folders for each employee reduces their chances, says Terry Bazemore Jr., principal cyber tester and COO of Ey3 Technologies in Upper Marlboro, Md. “The user would have read/write access to their own individual folder for saving the data to the shared drive, but not have access to anyone else’s folder on the drive,” Bazemore says. And the whole drive would be regularly saved — making it extremely difficult for a rogue employee to cause trouble even by wiping their own work.
- **Check the audit trails**. All your network processes, including your electronic health record (EHR), probably have audit trails that give a record of all accesses and actions. (If you’re not sure they do, you should check.) Some will have built-in filters that can quickly show when, for example, data movements, deletions or other types of activity have taken place. Gary Salman, CEO of Black Talon Security in Katonah, N.Y., recommends you review these trails at least once a month to see if anyone’s doing something suspicious.
- **Use a password management tool**. Also known as password managers, these tools give employees a way to sign into several accounts with a single password. In addition to being convenient, this also assures that employees never learn the actual passwords to sensitive accounts, such as your payers’. If you’re not using one, Salman suggests that you start — and if you do have one, considering extending its use so that your employees have fewer opportunities to get in when they’re not supposed to.

Resources

- ALXnow, “Former doctor’s office aide accused of computer trespassing after getting fired in Alexandria,” Oct. 9, 2021: www.alxnow.com/2021/10/06/former-doctors-office-aide-accused-of-computer-trespassing-after-getting-fired-in-alexandria/
- Careers Info Security, “Inside Job: Former Worker Allegedly Holds Records for Ransom,” Oct. 9, 2020: www.careersinfosecurity.com/inside-job-former-worker-allegedly-holds-records-for-ransom-a-15146
- Forbes, “A Hospital Employee Stole The Identities Of Dying Patients To Steal Covid Benefits, Feds Claim,” July 21, 2021: www.forbes.com/sites/thomasbrewster/2021/07/21/hospital-employee-steals-identities-of-dying-patients-for-covid-benefits-fraud-feds-claim/?ss=cybersecurity&sh=3478cd1b78e7
- 2021 X-Force Threat Intelligence Index, IBM: www.ibm.com/downloads/cas/M1X3B7QG

BACK TO TOP