An Often Overlooked Cybersecurity Threat: Employees, Current and Former

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

83% of Employees Admit They Have Access to Accounts of a Previous Employer

In February of 2022, Beyond Identity surveyed former employees in the U.S., the U.K. and Ireland. An astonishing 83% of them acknowledged that they maintained access to accounts of a previous employer. That alone is a horrific statistic.

Worse yet, 56% of the respondents acknowledged that they had used their access to harm their former employer. If they were fired, this number rose to 70%. 24% intentionally retained a password after their departure.

74% of employers report that they've been harmed by an employee getting past their digital security.

Anecdotally, when we perform an assessment for a new client's network, we invariably find dead accounts for long gone users, and all sort of indications that access to the network has not been carefully monitored. These are very foolish cybersecurity errors.

What do Former Employees Still Have Access to?

These are the worrisome answers of former employees to the survey:

- Old email account – 35%
- Work-related materials on a personal device – 35%
- Company social media accounts –31%
- Software accounts – 31%
- Shared files or documents – 31%
- Account with a third party system – 29%
- Other employee's email account – 27%
- Back-end of employer website – 25%
- Access to company's financial information – 14%

The All Important Out-processing Checklist

Every law firm should have an out-processing checklist, so they can veify that all digital access has been terminated – but many have no such checklist. This is borne out by the fact that only 50% of respondents were asked to return company devices (really???) and only 41% were asked to return digital tokens. Just 35% deleted or reset their accounts.

You don't have to create a checklist from scratch. All law firms should be members of the Society for HR Management – they have a wealth of wonderful information and templates. And yes, they do have a "Checklist: Employee Termination" which can be found at https://www.shrm.org/resourcesandtools/tools-and-samples/hr-forms/pages/termination_checklist.aspx.

The most common out-processing actions are:

- Wiping personal information/documents from all company devices
- Taking back security key or tokens
- Taking back company devices
- Changing passwords for all accounts employees had access to
- Deleting or resetting employee accounts
- Exit interviews
- Setting up email forwarding to someone else in the company
- Taking back company credit cards (and be sure to close that individual's company account)

It's Not Just After Termination That Employees are Dangerous

In the legal world, it is not uncommon for employees to collect data for a future employer while they are still employed by you. Because we do digital forensics work, we have often analyzed evidence of this activity and have offered testimony about it in court. Disgruntled employees have been known to do damage to the network long before they are fired. What mechanisms do you have in place to prevent that?

There is software these days that looks specifically for anomalous activities and sends alerts to a designated person to investigate those activities. Very often, the software picks up a large amount of data being sent outside the network or being copied to some external device such as a flash drive. You can utilize software such as SolarWinds Server & Application Monitor as a file tracking tool. Employee monitoring software such as Teramind, InterGuard or ActivTrak ups the game a bit by giving you vision into a specific employee's activities. Obviously, there are legal ramifications when monitoring employees, especially running in a stealth mode.

Attorneys planning to depart the law firm have been known to transfer vast amounts of data to their own personal devices, intending to take clients with them. Never a pretty outcome when that happens – not only are legal ethics often violated but employment contracts frequently contain a non-compete provision for a limited amount of time and with a specified geographical reach.

What do Employees Take with Them Before They Leave?

31% take coworker contact information, which may or may not be innocuous. 27% take company ideas, which is definitely not innocuous. 25% take contact information for clients, 24%

take company financial data, 24% take process related documents, 24% take passwords and 14% take pay stubs and tax information.

As you can see, there is a lot of data leaving with your employees. And yet, when companies do their off boarding, an IT specialist is only involved 9% of the time, which strikes the authors as downright crazy.

Cybersecurity Awareness Training

In a previous column, we talked about the critical need for cybersecurity awareness training. Without doubt, there are employees who wish their employers harm as outlined above. But the vast majority of employees simply are not educated about the accidental errors they are prone to making and the consequent harm to their employers.

They need regular training in spotting phishing emails/texts, social engineering, vishing, business email compromises, wire transfer protocols (you do have those, right?), why multi-factor authentication is so invaluable, encrypting confidential data, creating good passwords, managing their passwords – and the list goes on. Twice a year training is preferred but start with at least annual training. If Russia gets serious about increasing cyberattacks on the U.S., as our government now believes it will, you may get increasingly motivated to up your game.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* mmaschke@senseient.com.