# THE ENEMY WITHIN: Role of the Malicious Insider

Some of the most dangerous cybersecurity threats aren't outside your organization – they could be on your payroll, say Brunswick's **RIA THOMAS** and **WENDEL VERBEEK**

## "I'VE BEEN PASSED OVER AGAIN?"

"What do you mean we are through? I've committed 25 years to this company."

"Do people know how little this company actually cares?"

Those questions and cybersecurity may appear to have little in common. Yet a sense of injustice, boredom, revenge and financial vulnerability, including in their personal lives, can lead a trusted employee to break his or her contractual bonds of loyalty, steal critical data or disrupt the operational functions of a business.

The rising penchant to share one's hopes and frustrations over social media can draw an employee into the sights of organized crime elements, spy agencies, hacktivists and even terrorist organizations. It's well known that an employee can inadvertently click on a link inside a would-be invader's email. Yet a growing concern is the individual who has access to his employer's network or critical data and bears a deep-seated desire to cause damage.

The malicious insider may be found not only among employees but also contractors, vendors and anyone else with access to a company's systems or data. The risk encompasses not only individuals currently engaged with the company but also those whose relationship with the company has ended, voluntarily or otherwise. According to the 2017 Insider Threat Spotlight Report produced by Information Security, a LinkedIn community of more than 300,000 cybersecurity professionals, malicious data breaches are seen as the third-largest insider threat, just behind inadvertent and negligent data breaches. The 2017 Report is based on a comprehensive survey of more than 500 cybersecurity experts across many industries.

It can be difficult, culturally, for companies to admit that the threat may lie within, not merely from a naïve employee but from a trusted team member determined to wreak disruption, damage and destruction.

### What can be done to address or minimize this threat?

According to the 2017 Insider Threat Report, 74 percent of organizations feel vulnerable to insider threats, yet less than half of them have the appropriate controls in place to prevent an insider attack.

By controlling and managing access to data and systems, and by closely monitoring it, companies are hoping to gain early alerts to potential breaches. Careful monitoring may also assist in forensically mapping unauthorized access in the event of a major cyber attack.

Some employers have also begun to rely on technical oversight of their employees' behavior on company systems as well as social media platforms. These measures may include monitoring what an employee shares online about his or her employer or job. It may also involve automated reviews of what is emailed to addresses outside of the organization, and what is printed, by whom and in what quantity. Some may view this type of oversight as a violation of employee privacy; others may argue that expectations of privacy can blur at the edges of many confidentiality requirements placed on employees.

Regardless, employees need to understand what is expected of them. To earn loyalty and maintain open lines of communication, a company must be clear about employee responsibilities as well as what's at stake.

### What do you do when it happens?

Let's say you learn that confidential customer or other sensitive internal data has walked out the door in the hands of a disgruntled employee. Or that an employee has changed critical information in systems that risks destroying IP or bringing systems to a halt.

Your response can have a greater impact on reputation than the incident itself. When a potential loss, manipulation or disruption is

ILLUSTRATION: DAVID PLUNKERT

discovered, your technical team must quickly identify the scope of the damage.

It is then critical to identify the internal stakeholders. Who needs to be notified? Who can help determine the operational, financial and reputational implications? You will want a coordinated effort from the Cyber/IT teams, Corporate Communications, Human Resources (HR), General Counsel, Corporate Security, Key Business Unit Leaders and possibly others.

HR, for example, can determine whether any previous issues or concerns ever arose with a particular employee. Also, how closely does that employee work with others in the business – could anyone else be implicated or aware? Has the suspected employee completed all required data security training, as well as any other compliance requirements?

Ultimately, you want to have a clear plan in place to communicate the matter to executive leadership, the board, other employees and external stakeholders, including customers, law enforcement, partners, media, regulators and the general public.

You want agreed-upon principles designed to help avoid a crisis that might affect revenue, valuation and your overall corporate reputation. You will need a process that helps you determine when and how to:

**Acknowledge/Apologize** At a senior level, show empathy and demonstrate how the company is prioritizing the issue.

**Reassure** Commit to transparency as you gain clarity on the issue, and offer resources to help affected stakeholders.

**Learn** Make commitments to improve systems, training and/or culture to protect customers, employees, shareholders, partners and the general public. Illustrate externally the steps you are taking.

It is difficult to predict what would trigger someone to turn on his or her employer. But having a detailed plan in place can help reassure your whole organization that you are taking the necessary preventative steps.

**RIA THOMAS,** a Partner, leads Brunswick's cyber offer for the UK and Europe. **WENDEL VERBEEK,** a Director, focuses on crisis preparedness, cybersecurity and privacy. Both are based in the firm's London office.