Insider Threats: Why They Happen, and How to Prevent Them

In 2014, Sony was ostensibly held ransom by North Korean attackers calling themselves the 'Guardians of Peace' in retaliation against anti-DPRK film *The Interview*. The incident made headlines around the world, along with chilling images left across company screens depicting a skeleton and links to the publicly leaked data.

It was a sensation which gave *The Interview* more attention than it ever earned through marketing. An international caper that played out like a movie, it hit all the right notes: political intrigue, high-stakes technological savvy, vigilantism, and just a touch of terrorist phobia.

THE PLOT THICKENS

But North Korea might not have done it. In fact, evidence has mounted over time that the whole thing was pulled off by a disgruntled employee within Sony Pictures possessing a flair for the dramatic, and the good sense to cast suspicions on an easy target.

Security researcher Kurt Stammberger along with many others made the following case: "[Sony] was essentially nuked from the inside. We are very confident that this was not an attack master-minded by North Korea and that insiders were key to the implementation of one of the most devastating attacks in history." For its part, the DPRK – rarely one to refuse dubious credit for ingenuity – disavowed the whole thing with a shrug of annoyance.

Stammberger's assessment has been controversial, and the FBI rejected it after due consideration. But the researcher from security firm Norse nevertheless sheds light on an increasingly important issue: insider threats.

THE BIGGEST DATA THREAT

Research conducted within the last few years shows that the majority of cyber-crime and data breaches can be pinned on parties abusing their access to an organization's internal systems and processes. This is unsurprising: just as FBI statistics indicate that most violent crime is committed by acquaintances of a victim, it stands to reason that the biggest threats to an organization come from its own personnel.

In 2018, Ponemon Institute shared its findings based on interviews across 700 organizations and estimated that the average cost of an insider breach comes to **$8.7 million dollars.** Not only are such incidents financially devastating, but they also represent a significant risk to national security when they occur in government agencies.

703.729.9022 | www.mathcraft.com | info@mathcraft.com
44121 Harry Byrd Hwy, Suite 200, Ashburn, VA 20147

TYPES OF INSIDER THREATS

Insider threats come in a few different flavors, and understanding them is key to managing best practices for prevention:

- **Non-malicious error –** In most cases, insider threats do not involve any deliberate intention to subvert, damage or harm an organization. Error comes in many forms, from including non-organizational contacts on a sensitive internal email, to using public WiFi without a VPN or other form of data protection/encryption, to leaving hard drives with sensitive data in non-secure locations where they can be easily stolen. Mistakes like these can represent reckless lack of caution, or simply an honest misunderstanding of their seriousness.

- **Opportunistic exploitation –** Unscrupulous employees more technologically skilled than their management have every incentive to find and exploit various security holes inside an organization. There is a nearly limitless number of ways to profit from such holes, and there is every reason to believe that those who left them will fail to ever notice what is happening behind their backs.

- **Disgruntled employees –** Perhaps the most dangerous kind of inside threat is an employee with a chip on their shoulder. Whether it involves a raise dispute, human resource conflict or termination, a spiteful employee is motivated by vengeance rather than personal gain, and therefore has less interest in flying under the radar. That vengeance may involve freezing an organization's entire network, as former systems admin Christopher Grupe did to Canadian Pacific Railway after his termination.

PREVENTING INSIDER THREATS

As the industry becomes more conscientious of insider threats, organizations are tightening down security measures both preventative and reactive. Fortunately, there are many ways to mitigate the risk of internal breaches.

1. **Better employee training –** Teaching people to wash their hands can prevent the spread of disease. Training and enforcing basic security protocols can prevent million-dollar losses. Ensure your personnel understand data sensitivity and the risk of breaches, and act in responsible ways.

2. **Better awareness in management –** There are increasingly fewer excuses for managers to not understand their organizations' systems and security practices. Preventing opportunistic hijinks is as much a matter of knowing where they might occur as it is spotting them when they happen.

3. **Better security –** This one's a no-brainer, but it has to be said. Federal agencies are being held to higher standards ever since Executive Order 13587 mandated certain security practices, creating a demand for infosec contractors. Thankfully, those services are available to the public and private sector alike.

4. **Better employee oversight –** Keeping tabs on employees is especially important for preventing the more vindictive strain of insider threats. In some cases, an employee may have good reason to be angry. Keeping an open line of contact and investing in human resources can prevent bad-blood and raise awareness of danger when bad-blood starts to develop.

MathCraft Security Technologies offers a robust product line of NISPOM-compliant security applications for cleared contracts and enterprises. Our solutions are carefully engineered to improve security processes, giving Facility Security Officers (FSOs) and employees the comprehensive tools that they need to manage data, monitor visitors, and automate workflows. For ultimate convenience, they are also available on-premises or via the cloud.

MATHCRAFT SECURITY TECHNOLOGIES, INC.

Deltek Partner Marketplace

703.729.9022 | www.mathcraft.com | info@mathcraft.com

44121 Harry Byrd Hwy, Suite 200, Ashburn, VA 20147

www.deltek.com/en/partners/mathcraft-security-technologies