Harvard Business Review

The Biggest Cybersecurity Threats are *Inside* Your Company

When security breaches make headlines, they tend to be about nefarious actors in another country or the catastrophic failure of technology. These stories are exciting to read and easier for the hacked company to admit. But the reality is that no matter the size or scope of a breach, usually it's caused by an action, or failure, of someone inside the company.

The role that insiders play in the vulnerability of all sizes of corporations is massive and growing. In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actions.

IBM Security research also found that healthcare, manufacturing, and financial services are the top three industries under attack, due to their personal data, intellectual property and physical inventory, and massive financial assets, respectively. However, while industries and sectors differ substantially in the value and volume of their assets and in the technology infrastructures they have to manage and defend, what all businesses have in common is people — all of whom have the potential to be an insider threat.

Before addressing the threat, it's helpful to understand the primary types of insider risks:

- **We're only human, and at exactly the wrong time.** Human error is a major factor in breaches, and trusted but unwitting insiders are to blame. From misaddressed emails to stolen devices to confidential data sent to insecure consumer-grade systems, mistakes can be very costly. The riskiest of these are well-meaning IT admins, whose complete access to company infrastructure can turn a small mistake into a catastrophe.
- **A few people leak the passwords.** With these trusted but witting insiders, it's the thought that counts. Malicious employees whose intent is to steal or damage are a very real risk. Some steal competitive information, some sell data or intelligence, and some just have a vendetta against the organization.
- **A wolf in the clothing of John from accounting.** Cyber criminals are experts at hijacking identities. Some accomplish this by compromising an employee system through malware or phishing attacks. Some leverage stolen credentials, especially by gleaning data from social networks. In many cases attackers can increase a hacked user's access within a system, leading them to even more sensitive information.

The most dangerous aspect of insider threats is the fact that the access and activities are coming from trusted systems, and thus will fly below the radar of many detection technologies. Particularly in the latter two categories, malicious actors can erase evidence of their activities.

Based on the success of these types of attacks, they seem to represent a perfect crime. And in some organizations the challenge of identifying these rogue elements has resulted in attempts at "zero trust" environments.

But security teams have another formidable adversary: reality. While restrictive security policies may seem to be a valid strategy, they impede productivity, hamper innovation, and frustrate users.

Fortunately, analytics and the rise of artificial intelligence make spotting potential insider threats easier and less intrusive. However, even with advances in technology, managers need to be aware of what to look for and how to focus their security efforts to get the greatest returns on protection:

- **Focus on the right assets**. Bad guys want what you value most, what we call your businesses' "crown jewels." Identify the most-valuable systems and data, and then give them the strongest defenses and the most frequent monitoring.
- **Apply deep analytics.** Humans are creatures of habits: They come to work at the same time and do familiar tasks. The same can be said for how they use and interact with technology. Deep analytics and AI can uncover deviations in behavior at the level of individual employees, which can make it much easier to spot indications that systems have been compromised. We recently helped a customer collect and analyze terabytes of such data, and within 15 minutes they saw violations of policy that they didn't know existed.
- **Know your people.** Understanding the users who hold the potential for greatest damage is critical. Addressing the security risks that these people represent, and the critical assets they access, should be a priority. In particular, monitor IT admins, top executives, key vendors, and at-risk employees with greater vigilance.
- **Don't forget the basics.** In security we love the newest tools. But getting the basics done well can make the biggest impact on insiders:
    - Applying software patches automatically closes that open window before a hacker can use it to access your network.
    - Enforcing strong standards for user identities and passwords means stealing credentials is that much harder.
    - Collecting all the data and forensics you can on every device that touches your network makes sure you're the first to know if you've been hacked, not the last.

  But forget technology altogether. User awareness programs are the key to educating insiders. Train your people, test them, and then try to trick them with fake exercises. These basics make a disproportionate impact, but they do require work and perseverance.

So, when you read the next salacious headline about some breach by an external hacker, remember that these attacks account for less than half of the breaches out there. And remember that the hacker probably used the identity of an unsuspecting employee to pull it off.

Take action to make sure your organization isn't the next one in these headlines.

Article by Marc van Zadelhoff, published September 19, 2016 at:
https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company