
**White Paper**

# Employees: Security's Biggest Risk Factor
**2/12/2018**

Mitigating risk is the primary defense for any organization. Risk management is the process of identifying threats, understanding the value of vulnerable systems, and determining the best course of action to protect each system resource. Most security professionals do everything right when defending against outside risks, but they forget the biggest risk of them all: employees. Employees are an organization's biggest risk factor, and social engineering hacks continue to play on people's inability to identify cyber threats.

## Identifying Employee Risk Factors

The first step in risk management is to audit the network for any vulnerable resource. Even a printer can be used for hacking, so don't disregard resources because they seem benign. If the resource has computing power and handles private information, it's a source for hackers.

For example, an employee has access to several printers in the office. Suppose the employee prints a document that contains sensitive information. A disgruntled employee could swipe the document off of the printer and take it home for future use. Another employee could throw away the document without shredding it first. This leaves the data open to a technique called "dumpster diving" where the hacker collects unshredded information from the outside dumpsters.

These are just two examples of employees adding to security risks, but there are several ways they can put your organization's data at risk. When auditing the system, don't just consider how a hacker can gain access from the outside. Always consider internal risks and apply mitigation techniques accordingly.

## Email: The Biggest Threat to Employee Credentials

The right phishing email fools even security professionals sometimes. The biggest threat to an organization is malicious executables attached to an email or a phishing attack by an outside hacker. It's also the most difficult for administrators to manage, because you can have the best antivirus in the world but it won't help when "Sally" the employee runs a zero-day keylogger on her PC.

Keyloggers are especially dangerous, because they allow the hacker to gain access to anything Sally types. It also sends her credentials to the hacker. The most difficult part for a hacker using a keylogger is to avoid firewall settings, but most firewalls allow port 80 traffic. Port 80 is the port used with HTTP to browse websites. The hacker can perform an HTTP POST submit and send the private data directly to his web server without any notifications or alert from network security defenses.

Phishing attacks can be just as damaging. Employees are tricked into giving the hacker their credentials that give them access to the network. Hackers are then able to log in as a legitimate user, which also avoids common network intrusion detection. In a recent hack on a Ukrainian power utility, a phishing attack was able to obtain high-level credentials that gave the hacker access to critical control systems. It left 80,000 users in Ukraine without power. The attack was embedded in a Word document that the phishing recipient opened and executed. The mistake gave the hacker remote control of the user's desktop.

**Disgruntled Employees are Also a Risk**

It's no surprise that disgruntled employees are a risk factor, but they are even more difficult to detect. Disgruntled employees usually damage system resources or steal data before they are terminated or resign.

AutoDesk recently suffered from corporate espionage when a disgruntled employee left the company and stole core company code. The code was then given to one of AutoDesk's competitors in China.

One way to deal with disgruntled employees is to require mandatory vacations. Some employers purposely rotate job functions between different staff members. When new staff members are placed in an alternative role, they can identify any strange behavior on the system. When staff members take over for an employee on vacation, any questionable activity within the system can be questioned.

Before any staff member leaves, it's imperative that the user account is disabled and any access revoked before they leave the building. If the user resigns unexpectedly, disable the account right away. Some companies even ask a user to stay home for their last two weeks at the company to limit the amount of risk. You can't completely protect against disgruntled users, but you can take the necessary steps to disable accounts and permissions to limit risk.

**Executives are the New, Favorite Target**

Educated users know the sign of a phishing email, but plenty of people still fall for phishing emails. Hackers send dozens of phishing emails to a target organization in the hopes that at least a few people will fall for the attack. The problem with this type of attack is that email servers filter out many threats, and low-level users don't have the access rights needed to gain useful permissions.

Hackers have turned to more targeted attacks against executives. Instead of sending hundreds of emails that will likely be filtered out by spam detection software, hackers can send just a few targeted emails to high-level executives. If just one executive falls for the attack, the hacker has high-level access to corporate resources. Obtaining this type of data is a virtual goldmine for an attacker who can then use the information to sell on the black market or sell it to a competitor.

Executives are also prime targets for keyloggers. The hacker can obtain credentials and even keystrokes as the executive types sensitive information into a document or email. For this reason, executive emails should be a priority when assessing risk.

**Mobile Devices and Man-in-the-Middle Attacks**
Laptops aren't the only mobile devices that increase risk. Users often use smartphones and tablets for work. They connect these devices to any Wi-Fi hotspot and they have instant access to the Internet. The problem is that the user doesn't know what Wi-Fi hotspot he just connected to. It could be an official café hotspot, or it could be the hotspot a hacker sets up on his own smartphone.

When the hacker is able to trick users to connect to his own hotspot, he can perform a man-in-the-middle (MitM) attack. A MitM attack is when the attacker can relay information back and forth between client and host while intercepting and reading the data. The client and host are completely unaware of the attack.

The company can avoid a MitM attack using encrypted communication between employee and web host. However, this does not protect the organization when the employee connects to a malicious hotspot without encryption. For instance, the employee could send email from a mobile device to an email server with unencrypted data. This would give the attacker the ability to eavesdrop on the email. This also includes any chat programs that don't use encryption. If passwords are passed using these methods, the attacker could gain access to the user's credentials.

**Security Awareness is the Biggest Risk Mitigation Factor**
User education is the best way to avoid risk. What's obvious to a professional in the industry is not so obvious to a user. Users need education on the signs and red flags in email and when using hotspots. With some education, they can become more aware of malicious emails sent to their account.

User education also helps detect disgruntled employee behavior. They feel more empowered to report strange activity on the network whether it's from external or internal attacks.

If your company stores sensitive information and you need a better way to avoid risk, educate users and beef up any current security software. The first step is auditing the network, and then you can work with employees to more safely secure valuable assets.