ipswitch

Secure. Control. Perform.

AN IPSWITCH EBOOK

Insider Threats and Their Impact on Data Security

Introduction

Organizations around the globe are well aware of the consequences associated with data breaches. Sensitive data that ends up in the wrong hands can be sold on the black market and eventually lead to identify theft. Typically, enterprise security focuses on safeguards to prevent hackers from penetrating the network and gaining access to this data. Although this is a good start, organizations often naively overlook the dangers of data theft initiated by an insider.

Insider threats take place when a trusted insider (current or former employee, contractor or business partners), with access to an organization's trusted data, either unknowingly or intentionally participates in activities that negatively compromise the safety and security of this information.

According to the most recent Clearswift Insider Threat Index (CITI) report, 74% of security breaches originate from within the extended global enterprise.

When further probed, 72% of global security professionals believe their Board does not treat internal security threats with the same level of importance as external threats. These are alarming statistics. The figure below outlines the most common internal security threats faced by organizations today.

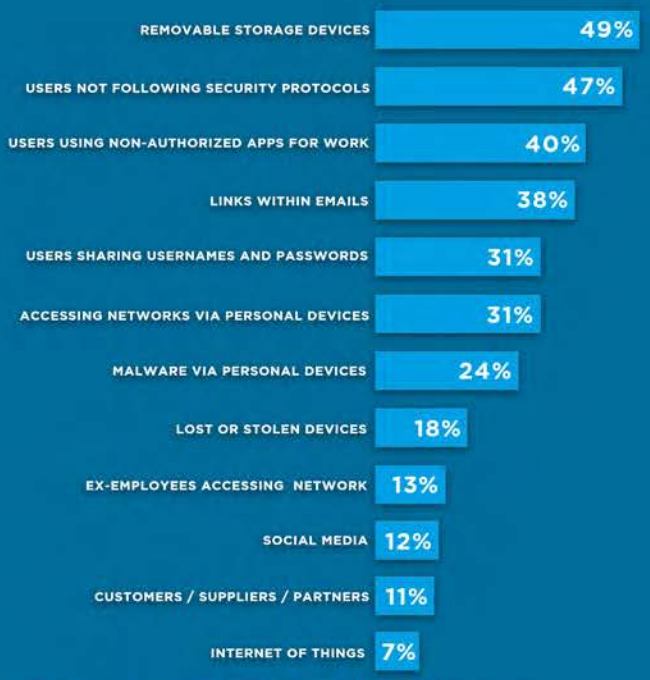


Figure 1: Biggest Internal Security Threats to Organization
Source: 2015 Clearswift Insider Threat Index

Figure 2: Mr. Robot
Source: USA Networks (http://www.usanetwork.com/mrrobot)

MR. ROBOT

Have you watched Mr. Robot on USA Networks? Mr. Robot portrays the epitomy of an inside threat in Elliot Aldreson.

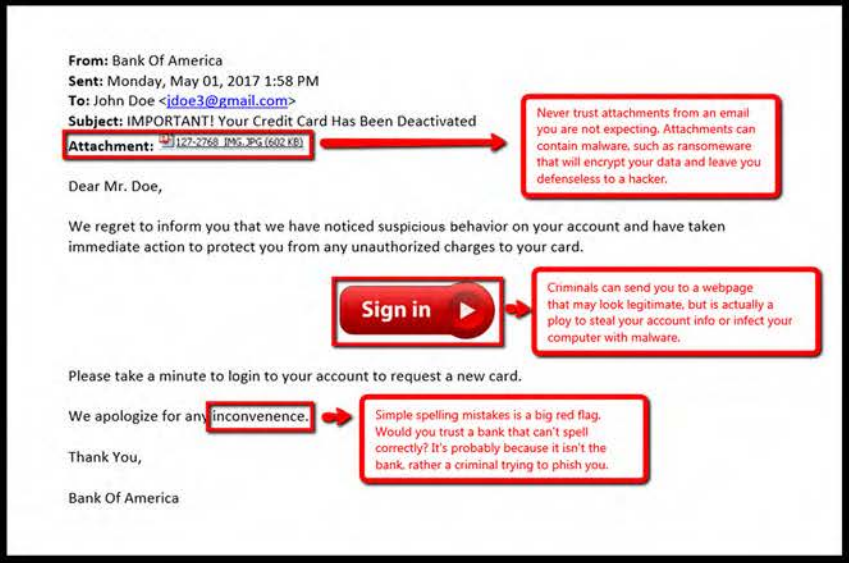
Elltiot is recruited by an anonymous group of hacktivists, run by a man known as "Mr. Robot".

During the day, Elliot works as a security engineer for the cyber security company, Allsafe. Elliot uses his insider knowledge of the company to help his hactivist friends commit cyber crimes from within the company, stealing its client's data and dsiclosing company secrets.

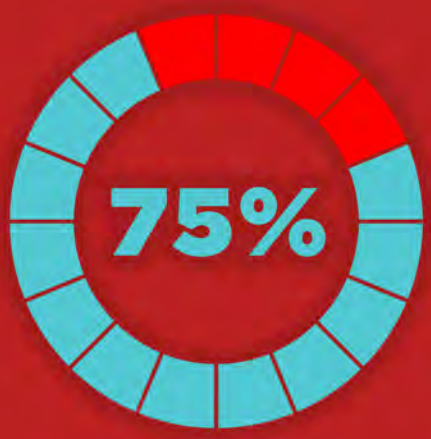
Of course Mr. Robot is an extreme example of an insider threat, but the show depicts very real vulnerbilities in today's business networks nonetheless. Although a fair number of internal data security breaches are committed by malicious insiders, a vast majority of insider threats are unintentional and are caused by individuals who inadvertently expose privileged information. Unintentional insider threats are usually the result of poor security practices such as leaving IT systems unattended or a failure to follow security protocols such as sharing system passwords with a colleague. These threats can be easily addressed by implementing robust security standards and protocols.

It is clear that in order to best safeguard the data integrity of an organization, IT teams should extend the implementation of existing data protection standards to address both external and internal security threats. Below are a couple of examples of common security threats that IT teams should look out for.

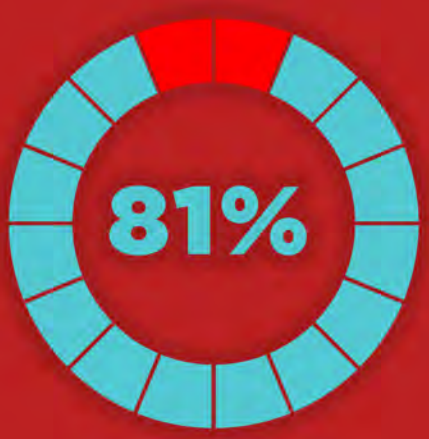
Posted notes with login information is an obvious issue. A criminal just needs to snap a pic through a window or see it on a desk. Also note the poor password.



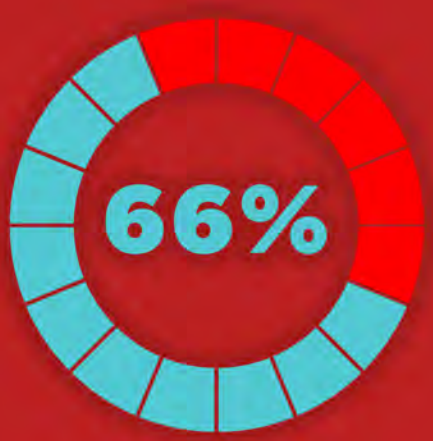
Email is never secure. Make sure your users know of the latest phishing scams. Training can be the best defense from a potential attack.



75% of breaches are from external actors vs. 25% internally.



81% of hacking related breaches caused by weak passwords.



66% of malware was installed via malicious email attachments.

Figure 3: 2017 Data Breach Investigation Report 10th Edition
Source: Verizon Enterprise (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/)

Most External Attacks are the Result of Internal Threats

As you can see from the data above, most data breaches are caused by external actors. Then why is it that internal threats are the most prominent? To make sense of this, you need to connect the dots.

Although most breaches are caused by external hackers, it's the business' employees who are inadvertently handing criminals the keys to the network. Weak passwords and malicious email are the major vectors of external attacks. But only if your users bite. In these cases, the users are the threat.

However, the problem with email goes beyond malicious email attachments. Sensitive data should not be sent by email unless it is encrypted both on the server and in transit. Office 365 and others offer this capability, but some services do not. It is important to be careful about which email services you are using.

Email Is Not Your Ally

We need not be reminded of the election that took place in 2016. Nonetheless, one of the key topics that during the election was of course Hillary Clinton's private email server which she was using to send and receive classified information.

Politics and espionage aside, the biggest issue with email is that email can be intercepted by a 3rd party without the sender or receiver's knowledge. You could have the most secure email server in the world, but it's useless once that data moves past the safety of your business firewall. The receiver of that data may not take security as seriously you, so who sees that email after you send it is out of your control.

Minimizing Insider Threats When Moving Data Outside the Firewall

In today's borderless enterprise, businesses need to be able to securely exchange sensitive information with external third parties on a regular basis. Moving sensitive data beyond the firewall exposes it to the potential risk of data interception and theft. A secure and reliable Managed File Transfer (MFT) solution can prove to be an invaluable investment for ensuring files are delivered to authorized recipients on time while enabling IT to monitor and capture all file transfer activity. When selecting tools to enable external data sharing, consideration should be given to capabilities such as account access, alerts and reports, integration with anti-virus and other security mechanisms.

Account Access

Unauthorized access to sensitive data is a clear breach in securing the information on your network. One way to ensure consistent and easy to manage control over which users have access to a given system is to integrate account access privileges with the active directory (AD) database. This enables the IT team to be able to control and monitor which employees have access to systems that house sensitive information. It also enables IT to be able to quickly disable or limit access to user accounts in the event of suspicious behavior or if an employee leaves the company.

Alerts, Dashboards and Reports

It is important for a managed file transfer system to be able to log all file transfer activity and trigger alerts that forewarns IT of malicious user behavior. Control and visibility into account access and file transfer events minimizes the potential damage that could occur in an insider threat attack. Tamper-evident audit logs ensure that even if an attack does take place, a trail of what happened is recorded and can be traced back to the offending individual(s).

Integration with Anti-Virus

A very common way to attack and infiltrate a system is by releasing malware into the network. Once a software virus is released, it can do a lot of damage and provide exposure to your most sensitive data before IT can get the situation under control. IT teams rely on up-to-date anti-virus software to help minimize the chance of such vicious attacks. Ensuring your managed file transfer system can integrate with network anti-virus software can help prevent malware that has been released into the network from affecting the FTP servers where data is stored.

Data Encryption

Data encryption plays a very important role when transferring data outside of an organization. Even if IT is able to limit authorized users from accessing databases that house sensitive information, it is also just as important to make sure data that is shared external to the company is not being read or modified. This process is also vulnerable to insiders who are looking to maliciously intercept and abuse protected information but it is often overlooked from a security standpoint. IT teams should ensure they have a managed file transfer workflow in place that ensures both data at rest and in-transit is encrypted. Data encryption prevents unauthorized users from misusing any meaningful data even if they manage to gain access to the underlying file store. It also ensures that the integrity of the data is not compromised in any way.

Multi-Factor Authentication

Multi-factor authentication (MFA) is another great layer of security that can help ensure only authorized individuals gain access to sensitive information. MFA is a multi-step verification process that ensures that the user is who he/she claims to be by requiring that they provide additional proof of who they are, most often in the form of a security code, when logging into a system account. The security code is delivered to an alternate source (phone, email, etc) that is linked directly to the individual. This additional security layer prevents employees from sharing passwords or from unauthorized users gaining access to sensitive data in the event that an account password is compromised.

Cloud Services

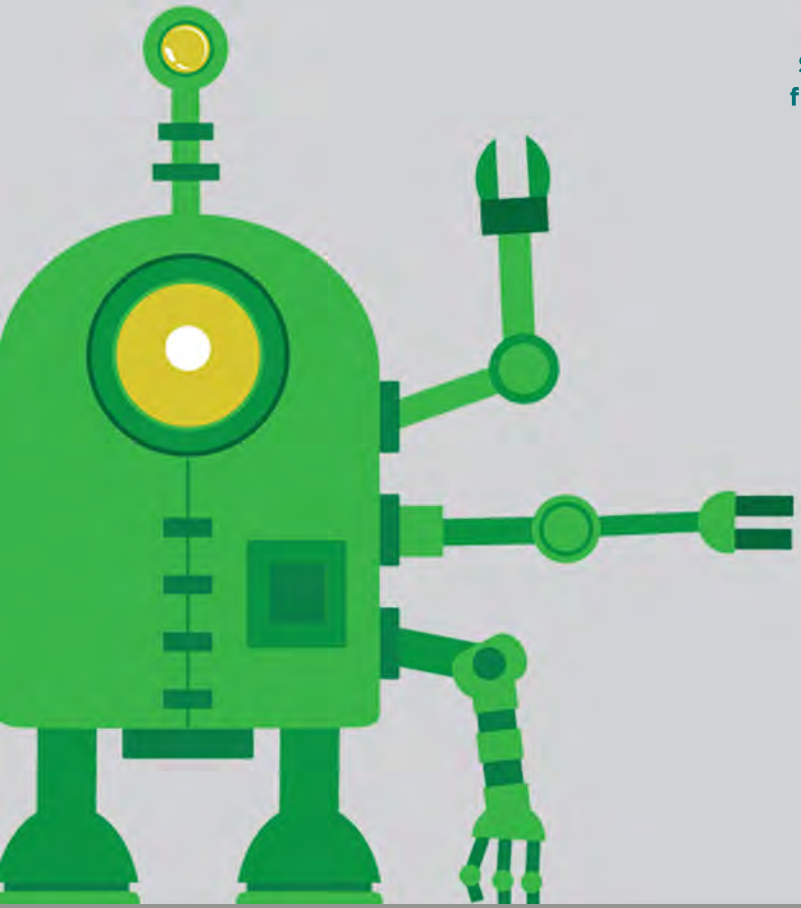
More and more applications today are being offered through the cloud. One distinct advantage of implementing a cloud-based SaaS solution for your file transfer activities is that it ensures all your software protocols are up-to-date. With a SaaS cloud-based offering, malicious insider attacks will have not have the same window of opportunity to access sensitive information. With an on-premise implementation, there is a distinct window of vulnerability between when software updates and/or patches are available and when they are scheduled and applied by IT to the network.

Automation

Automation creates a "hands off" data transfer methodology that reduces the chance of sensitive files ending up in the hands of unauthorized individuals due to (intentional or unintentional) scripting errors. A robust automation system enables IT to manage and track file transfer activity and quickly disable/stop certain transfers from taking place if fraudulent activity is suspected.

Figure 4: Intelligent Systems in Action
Source: Ipswitch (www.ipswitch.com)

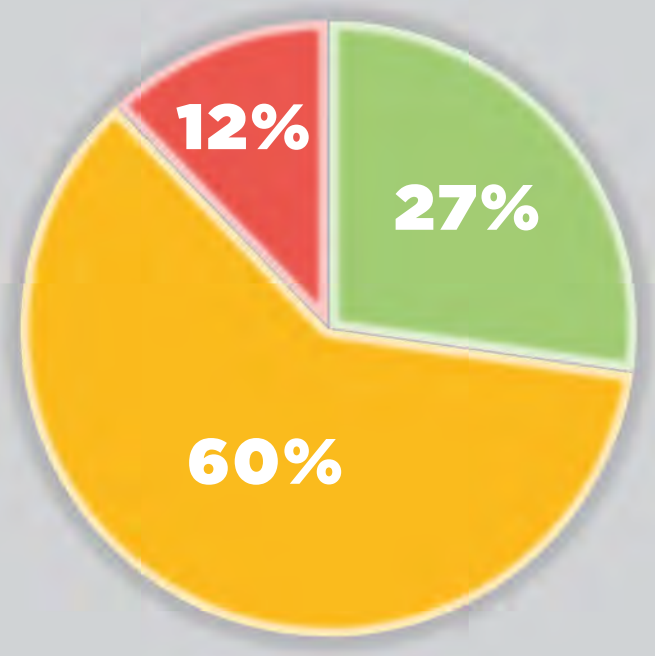
How would you rate your current capability in secure file transfer management and automation?



Strong and future proof

Needs strengthening

Already inadequate



Third Party Account Access

Insider threats are not just limited to contractors and employees. Today's businesses often develop close relationships with third party vendors and partners that require privileged access to information. Unfortunately, cybercriminals often leverage this access penetrate your defenses. This can often be prevented through the use of a 'gateway proxy' server which terminates inbound and outbound authentication and transmissions in the network DMZ (demilitarized zone) thereby prohibiting external access to your trusted network. Third party accounts can be further controlled by implementing least-privilege permissions and capturing an audit trail of all remote account access activity. In addition to these safeguards, third party accounts can be disabled or deleted once they are no longer needed.