



THE TOP 10  
MOST COMMON  
SECURITY MISTAKES  
BUSINESSES MAKE





# Table of Contents

## FOREWORD

Cybersecurity, a Major Challenge not to be Neglected.....3

## MISTAKE N° 1

Overlook Enforcement of a Strong Password Policy.....4

## MISTAKE N° 2

Use Outdated and Unpatched Software.....7

## MISTAKE N° 3

Use Vulnerable Edge Devices.....9

## MISTAKE N° 4

Neglect Email Monitoring and Protection.....11

## MISTAKE N° 5

Have Poor Visibility of the Network.....15

## MISTAKE N° 6

Mismanage Mobile Devices.....16

## MISTAKE N° 7

Neglect Access Privilege Policies.....18

## MISTAKE N° 8

Mismanage Directories.....19

## MISTAKE N° 9

Poorly Protect Cloud Services.....20

## MISTAKE N° 10

Use Inadequate Data Disposal Practices.....22

Common-Sense Security.....23

# Cybersecurity, a Major Challenge not to be Neglected

Cybersecurity is often seen as a technology problem that requires technology answers. With thousands of vendors selling tools to detect, prevent and recover from cyberattacks and global cybersecurity spending expected to top [\\$167 billion this year<sup>1</sup>](#), there is plenty of money being spent on solutions.

But the reality is that the vast majority of security problems result from human error, lack of knowledge and poor policies. Rather than acquiring new technology, organizations need to do a better job of using the tools they already have.

ESI tapped into its security team's many years of experience to develop this list of the 10 most common cybersecurity flaws they've encountered. Where appropriate, we've suggested technology solutions, but most of these gaps can be filled by developing robust policies, training users and following best practices.



**Roger Courchesne**

Director - Internetworking & Security Practice

ESI Technologies



## MISTAKE N° 1

# Overlook Enforcement of a Strong Password Policy

This the number one most common cybersecurity mistake, and also the easiest one to correct. Despite years of warnings about the importance of choosing passwords composed of random strings of characters, many people persist in using names of family members, birth dates, sequential number strings and other easily guessed codes.

Meanwhile, the software that criminals use to crack passwords is constantly improving.

Even brute-force algorithms – which simply run through combinations of random characters until a successful match is found – can process up to 350 billion guesses per second.

The statistics on password failures are alarming. An analysis of 11 million stolen passwords for cloud services conducted by [Skyhigh Networks](#)<sup>2</sup> found that just 20 character strings constituted 10.3% of all passwords on the list.



[Another analysis](#)<sup>3</sup> of 130 million passwords stolen in a hack of Adobe Systems in 2013 found that 5 passwords composed of sequential numbers protected 3.2 million accounts.

An equally dangerous practice is to use the same password across multiple accounts. Billions of passwords have been stolen in breaches over the past few years. An attacker who can compromise one account with a stolen password can frequently break into numerous other accounts held by the same user.

There are good reasons why people make these mistakes. Memorizing or writing down different passwords for each account is laborious and error-prone. Storing them in an electronic document provides little protection unless the document is encrypted.

A better option is to use one of the many digital password managers that are available at little or no cost. These products store passwords in encrypted vaults, automatically fill forms and can even preserve credit card and sensitive personal information. They can also suggest passwords that are all-but-impossible to crack. Users need to remember only one password to get access to their entire vault.

**59% of users admit  
re-using passwords in  
all their accounts.**

Security Boulevard, May 2018<sup>4</sup>

# Implementing Corporate Best Practices

Organizations can help enforce good password security with a few basic procedures.

1

Require that default passwords be immediately changed whenever new devices such as network equipment are installed. Leaving defaults in place on a router, for example, can enable an attacker to easily gain access to an organization's entire network.

2

Set the standard policies that users must follow, such as changing passwords for business-critical applications every three months. Most directory services and cloud applications enable administrators to force password changes on a pre-set schedule. Using password managers makes the process easy.

3

Provide employees with guidance on good password selection. In general, the longer the choice the better. Password-cracking software has become so sophisticated that experts now say a minimum length of 13 characters is needed. Character selection should be truly random; substituting "\$" for "S" and "1" for "l" doesn't fool the software criminals use. An increasingly popular practice is to adopt very long passwords such as memorable quotations or passages from books.

4

Encourage employees to use two-factor authentication (2FA) whenever possible. This technique, which supplements the password with a second form of verification such as a text message to the user's mobile phone, is being supported by more and more cloud services. According to [Symantec](#)<sup>5</sup>, 80% of breaches could be avoided by using 2FA.

# Use Outdated and Unpatched Software

Keeping current with software patches and updates is a significant challenge for even the most resource-rich enterprise IT organizations. For smaller companies on a limited budget the task is nearly impossible. A scan of the [National Vulnerability Database](#)<sup>6</sup> at the NIST illustrates the scope of the problem. Literally hundreds of patches are issued every month (which are not all critical) and impossible to keep up with. Those that do need to be applied must often be downloaded, tested and deployed in a rigorous manner that ensures that the fix doesn't break something else.

Unpatched software is a growing problem that has made headlines in recent security breaches. The devastating [Equifax 2017 breach](#)<sup>7</sup>, which revealed personal information about more than 140 million Americans, occurred when attackers exploited a vulnerability in an open source web application platform that had been patched months earlier. The respected [Ponemon Institute](#)<sup>8</sup> has estimated that 60% of organizations that suffered a data breach over a two-year period were the victims of an exploit of a known but unpatched vulnerability.

The prevalence of older PCs and operating systems is a significant problem. For example, as of early 2019, [NetApplications Inc. estimated](#)<sup>9</sup> that the installed base of Windows 7 still exceeded that of Windows 10, despite the fact that mainstream support for Windows 7 ended in 2015. In fact, more than 4% of PCs are still running Windows XP, which was introduced in 2001 and hasn't been updated in nearly five years.

## The Challenge of Mobile Devices

A further complication is the growing number of mobile devices that organizations must support. Laptops, smart phones and tablets in the field are difficult to corral, and traveling users are more susceptible to viruses introduced through channels like open Wi-Fi networks and USB sticks.

Keeping up with the patch deluge requires automation and priority-setting. Server administrators should subscribe to all relevant alerts from their strategic software providers and give priority to those patches deemed most critical. A good testing strategy is to use a second server in a virtual partition that mirrors the production environment.

### Endpoint Protection

Endpoint security is a more difficult problem. Organizations should audit all potential network entry points on a regular basis, ideally once per quarter. This includes desktops, laptops and network equipment connected to the public internet. Any systems running unsupported operating systems such as Windows XP or Windows 98 should be immediately removed and replaced. PCs running Windows 7 should be upgraded to Windows 10 with automatic patching turned on.

### Technology Solution

Fortunately, there are solutions that protect even against zero-day exploits. One example is Cisco's [Advanced Malware Protection for Endpoints](#)<sup>10</sup>. It uses a combination of pattern detection and a global vulnerability database to rapidly find and respond to malware infections. The solution goes beyond applying patches to inspect activity on endpoint devices on an ongoing basis for signs of anomalous behavior. When detected, AMP provides a built-in "sandbox" that isolates suspicious files for analysis without exposing them to other running software. If a file that appears clean upon initial inspection ever exhibits malicious behavior, AMP can deliver a full history of the threat's behavior for help in containment and remediation.

Even with these protections in place, there's no guarantee of immunity. For example, zero-day exploits are a type of attack that strikes at the same time new vulnerabilities are discovered. Because insufficient time has passed for a fix to be circulated, there is no way for organizations to apply patches in time.



# Use Vulnerable Edge Devices

Many organizations offer free Wi-Fi service as a courtesy to customers, but failure to attend to a few basic protections can turn that nicety into a security nightmare.

### The Risks of Wireless Devices

Public-facing Wi-Fi access points should never be connected or bridged to the corporate network. Organizations may overlook this basic bit of blocking and tackling for the sake of cost or convenience, but they do so at their peril. Adding password security to public access points is a weak protection for all the reasons noted in item 1 above. The better approach is to contract with a commercial Internet service provider whose network is independent of your own.

Most public Wi-Fi access points are unencrypted, meaning that data transmitted through them remains in plain text format. Cybercriminals can easily “sniff” this traffic to capture all packets that traverses the network. For this reason, employees, contractors and even customers should be cautioned against using public access points for business.

As endpoint devices proliferate, organizations struggle to maintain an inventory of all their potential vulnerability points of access.

One factor that contributes to this blindness is the ease with which individual devices can now create vulnerabilities without the knowledge of the IT organization. For example, many PCs and smart phone come with a default option to configure them as open wireless access points. Employees may use this convenient feature to set up ad hoc workgroups or save on wireless data costs but then forget to turn it off. Upon connecting at work, they essentially create an open on-ramp to the corporate network.

**Half of security professionals believe they are unaware of all the connected devices accessing their networks and 60% don't know when new connected devices come into the office.**

Pwnie Express  
Internet of Evil Things Report<sup>11</sup>

## Special-Purpose Websites

Another area of concern is temporary or special-purpose websites that connect to the business network without a full set of protections. This was an issue in the massive [JP Morgan Chase attack](#)<sup>12</sup> of 2014, which compromised information on 76 million households and seven million small businesses. The company had set up a public web server to support a road race and enabled employees to log on with their business credentials without encrypting or otherwise protecting the information. Attackers were able to use a security certificate stolen from a contractor to intercept traffic to the server, including login credentials.

A contractor's compromised login information was also a factor in the [Target Stores breach](#)<sup>13</sup> earlier the same year.

The contractor had been granted a level of privilege that attackers were able to use to install software on the company's point-of-sale systems that captured credit card numbers and other sensitive information.

## Technology Solution

Cisco's [Next-Generation Firewall](#)<sup>14</sup> is an excellent source of edge protection. It combines an intrusion detection and prevention engine with identity-based and device-aware security that operates at layer 7 to identify users content and applications on the network. Not only can administrators enforce security policies on every device, they can also block traffic from certain destinations and prioritize demanding traffic such as videoconferencing.

## The Danger of IoT

Unfortunately, the Internet of things will make matters worse. Organizations are increasingly installing devices like programmable thermostats, smart cameras and intelligent lighting systems and connecting them to their network. These devices may come with little or no security, making them easy prey for criminals. It certainly won't be the last. As a basic protection, change the default passwords on all devices added to your network, and use network segmentation to limit access to critical infrastructure and information.

## MISTAKE N° 4

# Neglect Email Monitoring and Protection

Despite security administrators' best efforts to enforce good password practices and plug holes in corporate networks, there's little they can do to protect users from their own mistakes. The inbox remains a most stubbornly persistent threat to security.

Statistics tell the story. [FireEye estimates](#)<sup>15</sup> that 91% of cybercrime starts with email. Verizon's [2018 Data Breach Report](#)<sup>16</sup> found that 92% of malware was delivered via that channel.

Ransomware, which was the fastest-growing strain of malware in 2017, usually begins its journey from an inbox.

### Increasingly Sophisticated Attacks

Email-based attacks have changed over the past few years as criminals have honed their ability to target messages. Spam filters are now so good that few users even see spam messages any more, but through a technique known as "spear phishing," criminals can bypass even the best controls.

A survey of 1,300 security professionals indicated that 56% of them reported that targeted phishing attacks were their main security threat.

CyberArk  
[Global Advanced Threat Landscape Report 2018](#)<sup>17</sup>

The root of the problem is trust. Email is such an essential utility to business professionals that it's easy for people to fall into the trap of believing that every message is genuine.

Spear phishing preys on this complacency. Criminals mine personal information from social media profiles and match it to email addresses. They might also scan a person's recent activity to find points that establish trust, such as membership in an organization or recent purchases. And they look at friend networks to find the names of people their targets already know.

Armed with this information, attackers can easily spoof the "from:" field of an email message to make it appear to be from a friend. Including a little personal information gleaned from a social media site puts the recipient's mind at ease.

The message includes a link to a malicious website that either installs malware or asks for login information. Spear phishing practitioners are so skilled today that even cybersecurity professionals have admitted to falling prey.

Email-borne attacks are extremely difficult to defend against because they are specific to each user on the network. A single click on an attachment or malicious link can unleash a flood of malware that quickly spreads throughout the organization.

Ransomware is a particularly noxious new factor. It instantly encrypts a user's hard drive and demands a ransom payment in cryptocurrency in exchange for the decryption key. Some forms of ransomware also copy themselves to other PCs on the network and encrypt them as well.







## Technology Solutions

Technology enabled by machine learning is also coming into play. [Cisco's Email Security](#)<sup>18</sup> suite provides added protection with a layered approach that monitors both inbound and outbound communications. The software use machine learning to quickly identify fraudulent senders, including those that are likely to evade even cautious users. URLs embedded in emails can be checked for validity and the reputation of sender domains checked against blacklists and public records.

Cisco also offers protection against domain hijacking, a common tactic of email attackers. Users are immediately notified if a domain has been compromised.

Another useful technology is [URL filtering](#)<sup>19</sup> which limits the destinations users can visit. Filtering enables administrators to control access to websites based upon information contained in a URL list. Companies can maintain a local URL list or cloud-based URL Feed services like [Cisco Umbrella](#)<sup>20</sup>, which monitors website content also at the DNS layer. While filtering doesn't guarantee that users won't click on malicious links, it can significantly limit the damage.

# Ways to Enhance Protection

Fortunately, defending against email-borne attacks is fairly simple. It consists of educating people about a few basic practices.

1

**Never click on links or attachments in email messages** unless you're absolutely certain about the identify of the sender. That information can be easily verified by looking at the email header, which is different than the "from:" field.

2

**Never send personal information** like financial account numbers or passwords by email. No reputable organization will ever ask you to do so.

3

If directed to a login page from an email, **verify that the web address is what's expected.** Attackers can construct fake web pages that look exactly like legitimate banking, commerce and social networking sites.

4

**Be judicious about what information you share** publicly on social networks.

## MISTAKE N° 5

# Have Poor Visibility of the Network

It took organizations an average of 191 days - more than 6 months - to discover a breach in 2017. That's unacceptable in light of the fact that a skilled intrusion team can typically gain access to domain administrator credentials in an average of 3 days.

2017 Cost of Data Breach Study

Ponemon Research

You can't prevent attacks from devices you don't see. Unfortunately, many organizations lack a comprehensive view of their networks. Perhaps they can see IP addresses, but they have little information about what those devices are.

Poor visibility increases the risk that attackers can penetrate a network and remain undiscovered for weeks or months, a metric known as "dwell time." During that period, intruders can siphon off large amounts of information in small, steady streams that evade detection.

### Information Sharing

The problem is made worse by the open nature of IP networks. The Internet Protocol was designed to make information freely discoverable, meaning that devices willingly share information about other devices on the same subnet, including such things as operating system versions and running applications. A cyberattacker can exploit this information to find unpatched software that can be exploited to take over additional machines.

### Network Segmentation Failures

Poor network segmentation practices compound the problem. Segmentation is a useful way for administrators to limit access to certain kinds of information by grouping devices into subnets with different permission levels. However, many organizations don't bother to create subnets, effectively exposing their entire network to anyone who can breach a single firewall. Conversely, over-segmentation creates complexity that can also expose vulnerabilities. For example, 30 subnets with 25 permission policies each creates 750 rules to administer. Errors and oversights are easily missed in such a complex environment.

### Technology Solution

A network visibility solution like [Cisco Stealthwatch](#)<sup>22</sup> not only gives network and security administrators a comprehensive view of the devices on their network but also monitors traffic to detect malware even in encrypted data streams. Stealthwatch can also recommend optimal segmentation strategies and maintain security policies for each subnet.

# Mismanage Mobile Devices

Nearly everyone now carries a smart phone, but many businesses are behind the times when it comes to treating them as part of their IT infrastructure. The “bring your own device” policies that dominated the early years of the smart phone revolution are dangerously inadequate to govern the use of today’s powerful devices.

Regardless of whether users bring their own phones to work or the company provides them, mobile devices demand the same security considerations as desktop and laptop PCs. In fact, they demand additional attention because of the ease with which they are lost or stolen, as some [70 millions](#)<sup>23</sup> are each year.

Mobile devices present some unique new security threats. Because of their built-in cameras and audio recorders, compromised phones can become listening and video recording devices without the user’s knowledge. Their built-in GPS also makes them vulnerable to location tracking, a feature that is particularly useful to criminals engaging in corporate espionage.

Mobile phone security is improving, but IT organizations shouldn’t rely on built-in features alone for protection. Researchers have shown that PIN codes and swipe patterns can be detected from up to 15 feet away and no biometric protection has been shown to be foolproof. A better practice is to use two forms of authentication.

But criminals don't have to gain physical access to a mobile device to do damage. Mobile malware is now a firmly established category, with more than 4,000 threat families and variants cataloged as of early 2018.

[McAfee Mobile Threat Report Q1, 2018](#) <sup>24</sup>



While some of these rogue programs make their way into legitimate app store channels, many are spread through phishing schemes that send text messages to unwitting users directing them to websites that plant malware on their devices.

Effective mobile security begins with sound policies that are communicated thoroughly. Basic steps include keeping devices up-to-date with the latest operating system versions and security patches, regularly backing up data and using encryption for data both on the device and in transit.

Users should avoid public Wi-Fi hotspots and never click on unknown links in emails and text messages.

## Technology Solution

Organizations can employ mobile device management (MDM) tools like [Cisco's Meraki System Manager](#)<sup>25</sup> to gain extra levels of protection.

For example, MDM administrators can monitor and diagnose all the mobile devices on their network as well as get an inventory of installed software. Security policies can be administered remotely, including disabling cameras, prohibiting screen captures and turning off automatic synchronization.

Devices can also be remotely locked or erased if stolen. Finally, MDM provides enhanced network visibility by giving organizations a complete inventory of all of their mobile devices, their status and location.

# Neglect Access Privilege Policies

Amid the pressure of day-to-day business, details are easily forgotten, or loose ends left untied. When those details concern access privileges, it's a problem.

Many end-users don't understand how file permissions work or don't pay attention to guidance the IT organization provides the result is that sensitive information can easily be left in the open for anyone on the network to see.

A recent [report by Varonis](#)<sup>26</sup> based upon a scan of 6.2 billion files across 130 companies dramatized the problem. Among its findings:

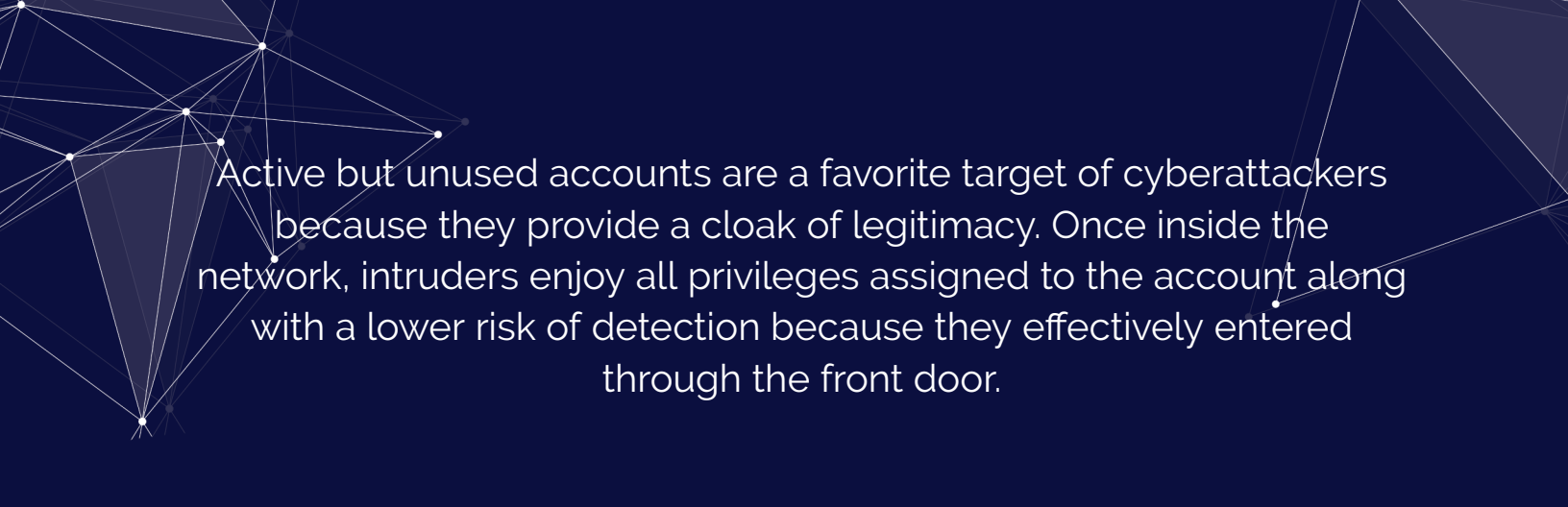
- 21% of all folders were accessible to every employee;
- 58% of companies had more than 100,000 folders in the open; and
- 41% of companies had no permission restrictions on more than 1,000 sensitive files.

These oversights are significant in light of the fact that about two-thirds of security incidents are caused by employee or contractor negligence, compared to just 22% by malicious parties, according to a [Ponemon Institute Study](#)<sup>27</sup>.

Lack of knowledge is the biggest culprit. Employees may be unaware of procedures for assigning permissions or may drop files into insecure folders thinking they're protected. Folders deep in a file system may contain permissions that aren't visible at higher levels, causing administrators to mistakenly assume that protections are in place.

Awareness and training are the best remedies. The IT organization should demonstrate how to assign file and folder permissions and convey best practices, such as assigning access at the group level and never to individual users. An even more secure approach is to limit creation of new folders to IT administrators, although that isn't practical in every case.

Technical solutions are available in the form of enterprise content management systems, which regulate access to and distribution of content throughout the organization. These systems often also include sophisticated workflow management capabilities that can streamline processes and enhance efficiency.



Active but unused accounts are a favorite target of cyberattackers because they provide a cloak of legitimacy. Once inside the network, intruders enjoy all privileges assigned to the account along with a lower risk of detection because they effectively entered through the front door.

## MISTAKE N° 8

# Mismanage Directories

When an employee leaves the company, managers are understandably more concerned about getting work done and filling the open position than deactivating access privileges. Unfortunately, over time this can create a big hole in the organization's defenses.

With people today posting their entire job history on social networks like LinkedIn, it's easy for hackers to identify candidates by looking for people who have recently changed jobs and whose credentials might therefore still be valid. They can cross-correlate that information with the billions of stolen user names and passwords available on the dark web to narrow down their list of candidates.

Turnover isn't the only vulnerability. Accounts are often set up for contractors and temporary workers without careful attention to access privileges.

Administrators either forget to shut them down when the assignment ends or leave them open in case the temporary worker returns.

The Varonis report cited above refers to these directory entries as "ghost accounts." Its survey found that one-third of accounts are enabled but unused and 65% of companies have more than 1,000 ghost accounts.

Other common directory-related problems include granting overly generous permissions and assigning group memberships without properly vetting access requirements.

To deal with the ghost account problem, organizations should designate a person within the human resources department to ensure that access privileges are revoked for departing employees. It's also a good idea to audit the list of accounts annually and remove any that are unused. Directory administration should be confined to a few individuals who are trained in best practices for the chosen directory service.

# Poorly Protected Cloud Services

## Data Encryption

Most software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) providers offer excellent security, but that doesn't mean customers should assume that the burden is lifted from their shoulders.

For example, IaaS providers may support data encryption but leave the responsibility for encrypting data and maintaining decryption keys in the hands of their customers. Or they may provide controls to prevent the downloading of information but leave that option disabled by default. Each provider has its own policies, and it's up to the customers to do their homework.

## Data Leak Prevention

User error is the most common cause of cloud security breakdowns. Assumptions that data is secure have led to numerous embarrassing incidents, such as [FedEx's early 2018 leak](#)<sup>28</sup> of more than 119,000 documents containing personal information that were left in plain-text format on an unsecured cloud server. Organizations should limit the number of cloud storage providers they use and apply administrative controls to limit what users can share and download.

It's usually dangerous to assume, especially when it comes to cloud services. Employees can walk down the hall to ask security-related questions of their IT administrators, but most people never even speak to the companies that provide cloud services. That can lead to dangerous assumptions about who is in charge of what.



## Password Selection

Poor password selection can leave applications and critical data exposed to anyone on the internet. Requiring the use of two-factor authentication can minimize this risk.

Users should also be educated about best practices for sharing cloud data. For example, sensitive data should only be shared with named individuals rather than through a global URL that enables edit access.

## Technology Solution

[Cisco's Cloud Security](#)<sup>29</sup> portfolio can automate much of this process by providing visibility into Internet activity, detecting and responding to threats and extending on-premises controls to applications running on public cloud infrastructure.

[Cisco Cloudlock](#)<sup>30</sup> provides a cloud-native access security broker that sits between software applications and users to monitor activity and enforce security policies.



## Use Inadequate Data Disposal Practices

Equipment that has reached the end of its useful life can be a significant security risk if proper disposal practices aren't employed. Many people believe simply deleting all the data on a disk drive or formatting the media is enough protection, but neither measure actually removes much data.

Rather, they remove pointers from directories, but leave up to 90% of the data intact and easily recoverable using special software. Even multiple formatting passes can still leave significant amounts of data in place.

IT asset disposal (ITAD) is a specialized discipline for destroying data. ITAD providers employ techniques ranging from erasure with high-powered magnets to physical destruction of media using machinery that grinds disk drives into powder. .

Professional services also provide a certificate of destruction that satisfies most regulatory inquiries.

Some can also refurbish equipment and recover some value through sale on secondary markets.

ITAD services can be expensive and aren't necessary in every scenario. Organizations should have a process for evaluating end-of-life equipment and identifying that which merits specialized handling.

This process should apply to any equipment that contains data, including servers, PCs, smart phones and USB drives.

# Common-Sense Security

Small business owners may think they're protected from cyberattacks because their size makes them an unattractive target, but 58% of malware attack victims in 2017 were small businesses, [according to Verizon](#)<sup>31</sup>.

Criminals assume that smaller companies are resource-constrained and lack the sophisticated detection and prevention technology of larger enterprises. While large organizations are well-equipped to withstand even large data breaches, the impact can be devastating on companies operating on thinner margins. Cyberattacks cost small and medium-sized businesses an average of \$2.2 million in 2017, [according to Ponemon](#)<sup>32</sup>.

Fortunately, paying attention to the 10 issues listed here can thwart the vast majority of cyberattackers.

To further explore the issue, contact us for a presentation.

[expertise@sitechnologies.com](mailto:expertise@sitechnologies.com)

**ESI Technologies**

[www.esitechnologies.com](http://www.esitechnologies.com)

1-800-260-3311

MONTRÉAL

TORONTO

QUÉBEC

1550 Metcalfe St., Suite 1100

Montréal, QC H3A 1X6

514 745-2524 1-800-260-3311

# Resources

- <sup>1</sup> <https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/>
- <sup>2</sup> <https://www.skyhighnetworks.com/cloud-security-blog/you-wont-believe-the-20-most-popular-cloud-service-passwords/>
- <sup>3</sup> <https://www.zdnet.com/article/just-how-bad-are-the-top-100-passwords-from-the-adobe-hack-hint-think-really-really-bad/>
- <sup>4</sup> <https://securityboulevard.com/2018/05/59-of-people-use-the-same-password-everywhere-poll-finds/>
- <sup>5</sup> <https://www.slideshare.net/cheapsslsecurity/vip-strong-authentication-no-passwords-infographic-by-symantec>
- <sup>6</sup> <https://nvd.nist.gov/vuln/full-listing>
- <sup>7</sup> <https://www.wired.com/story/equifax-breach-no-excuse/>
- <sup>8</sup> <https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf>
- <sup>9</sup> <https://netmarketshare.com/operating-system-market-share>
- <sup>10</sup> <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance-c45-731874.pdf>
- <sup>11</sup> <https://www.pwnieexpress.com/2018-internet-of-evil-things-report>
- <sup>12</sup> <https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>
- <sup>13</sup> <https://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html>
- <sup>14</sup> <https://www.cisco.com/c/en/us/products/security/firewalls/index.html>
- <sup>15</sup> <https://www.fireeye.com/offers/rpt-email-threat-report.html>
- <sup>16</sup> [https://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2018\\_Report\\_en\\_xg.pdf](https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf)
- <sup>17</sup> <https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018/>
- <sup>18</sup> <https://www.cisco.com/c/en/us/products/security/email-security/index.html>
- <sup>19</sup> <https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html>
- <sup>20</sup> <https://umbrella.cisco.com/>
- <sup>21</sup> <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SELO3130WWEN&>
- <sup>22</sup> <https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>
- <sup>23</sup> <https://www.awingu.com/what-is-the-true-cost-of-a-lost-mobile-device/>
- <sup>24</sup> <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf>
- <sup>25</sup> <https://meraki.cisco.com/solutions/emm>
- <sup>26</sup> <https://www.varonis.com/2018-data-risk-report/>
- <sup>27</sup> <https://securityintelligence.com/media/2016-cost-data-breach-study/>
- <sup>28</sup> <https://www.zdnet.com/article/unsecured-server-exposes-fedex-customer-records/>
- <sup>29</sup> <https://www.cisco.com/c/en/us/products/security/cloud-security/index.html>
- <sup>30</sup> <https://www.cisco.com/c/en/us/products/security/cloudlock/index.html>
- <sup>31</sup> <https://enterprise.verizon.com/resources/reports/dbir/>
- <sup>32</sup> <https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html>