The Current State of Email Security

Office

Microsoft

Table of Contents

SECTION 01

SECTION 02

SECTION 03

SECTION 04

State of the Industry

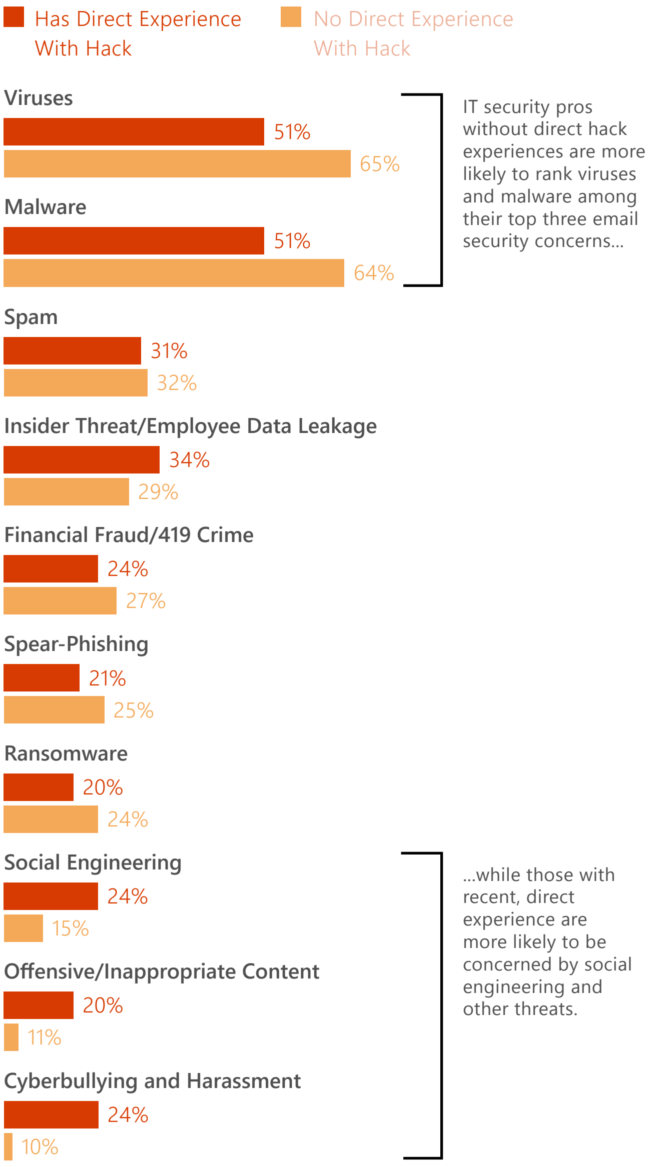
Today's businesses rely heavily on email to communicate with clients, partners, and colleagues. But research suggests that organizations are lacking when it comes to protecting themselves against the increasing number of customized and complex attacks.

When polled by Mimecast, 83% of IT security managers said they see email as a primary source of attack, yet 65% claim they aren't fully equipped to resolve the risks associated with email threats. Respondents' perceptions of primary security threats also appeared to change based on having experienced a successful breach. However, viruses, malware, spam, and insider threats remain the top concerns for both groups, both with and without breach experience.

Similarly, security vendor Proofpoint reports that email continues to be the primary threat. In the first quarter of 2016, malicious email volume increased by 66% from the previous quarter, with attachments as the preferred delivery method over embedded links.

Concerns Posed by Different Email Threats

% Who Ranked them in their Top 3 Concerns



IT security pros without direct hack experiences are more likely to rank viruses and malware among their top three email security concerns...

...while those with recent, direct experience are more likely to be concerned by social engineering and other threats.

"Business Email Threat Report," 2016, Mimecast

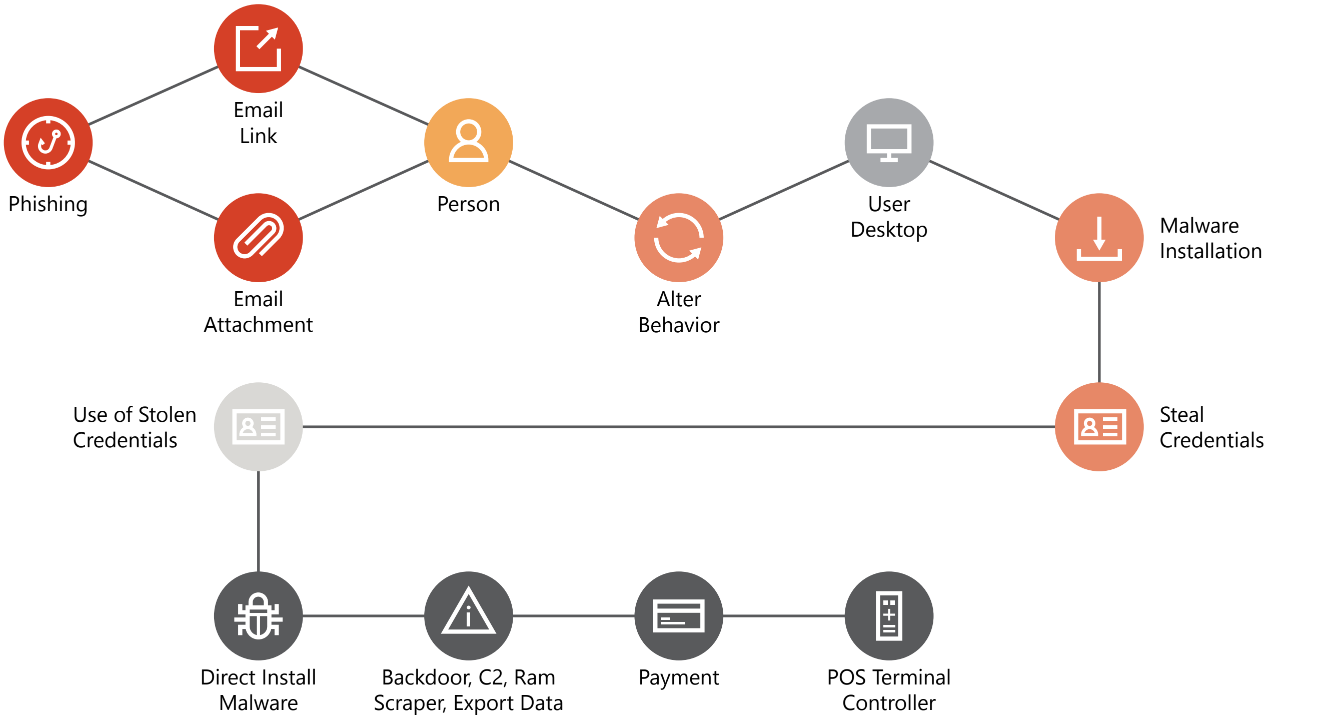
Thanks to cloud computing and ubiquitous broadband, today's employees can usually send and receive email from any location and from any device—both a blessing and a curse. This complicates email security, as any feasible solution must cater to multiple platforms and devices.

Hackers are professionals at what they do, and they don't follow any set rules. In addition to more common security threats, email is often a vehicle for more sophisticated attacks. Phishing, for example, uses email to gain network entry, which could lead to malware installations, credential theft, and more. While email remains a primary threat, we cannot ignore that email security must be part of a larger cybersecurity defense policy.

Today, mitigating security risks requires that companies take a holistic approach to finding the right solution by considering the mindset of the attacker, the various threats present, and current trends. Whether your chosen email solution is located in the cloud or on-premises, assessing both external and internal threat risks is essential.

This report explores email security threats' most common delivery methods and identifies their risks to your organization, offering effective solutions to both internal and external threats and how to implement them.

Birth and Rebirth of a Data Breach



"Data Breach Investigations Report" 2016, Verizon

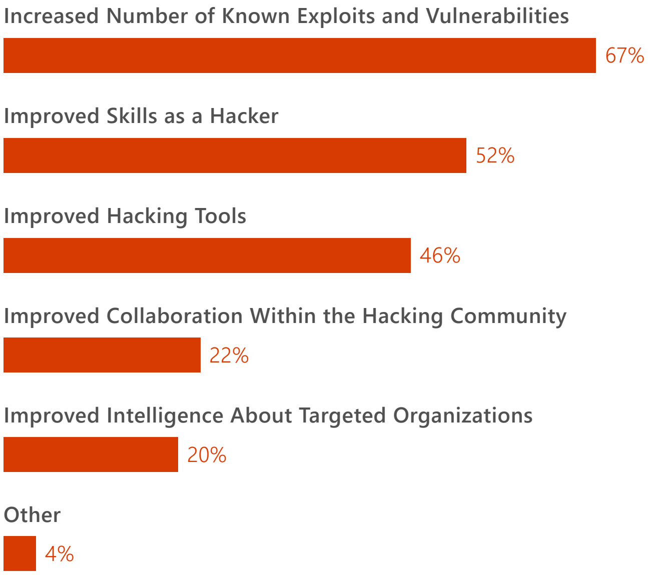
External Threats

Given its high usage, it's no surprise that email remains a primary target for those who wish to disrupt business operations or acquire confidential data. But what exactly motivates attackers to do what they do? In a Ponemon Institute survey of more than 300 technically proficient hackers, 69% claimed financial motivation, with 72% confirming that they select the easiest target first.

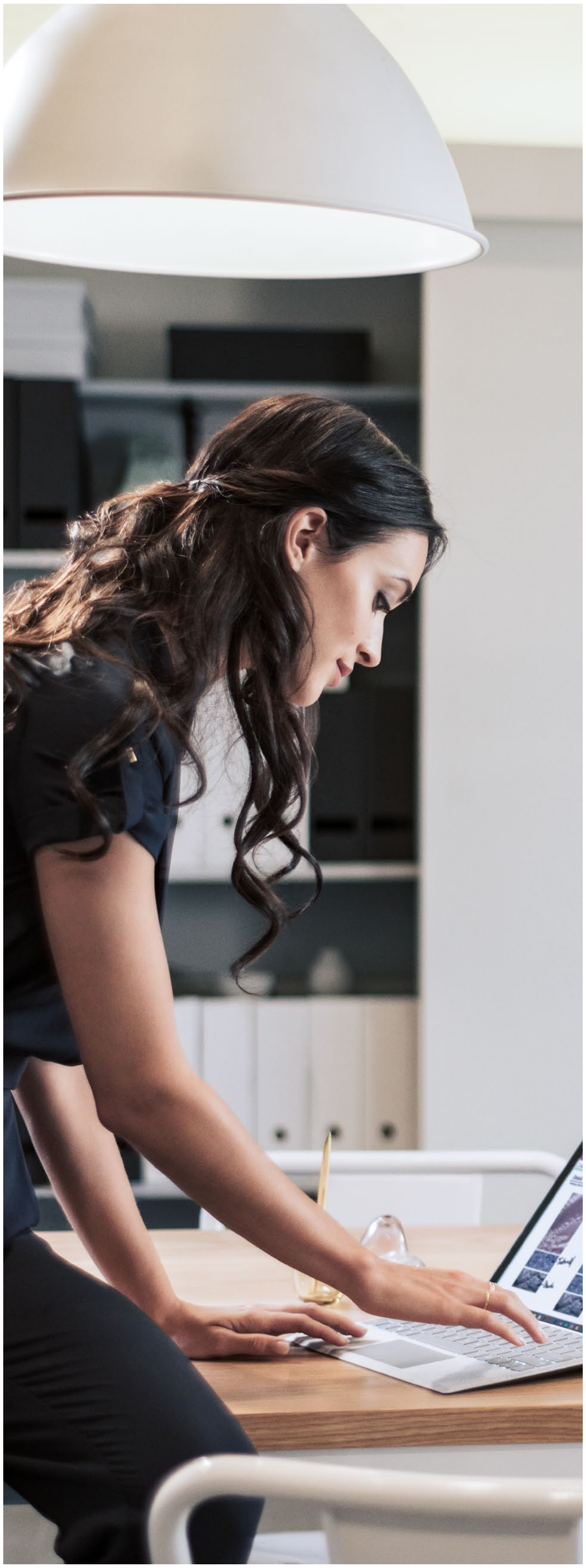
What stops a hacker in his or her tracks? Looking for easy targets, 69% of the Ponemon survey respondents would quit an attack if the target had a strong defense. But the reality is that hackers continue to become more agile; 67% of surveyed respondents can more swiftly facilitate attacks due to an increase in the number of exploits and vulnerabilities.

Why Time to Plan and Execute an Attack Has Decreased

More Than One Response Permitted



"Flipping the Economics of Attacks," 2016, The Ponemon Institute

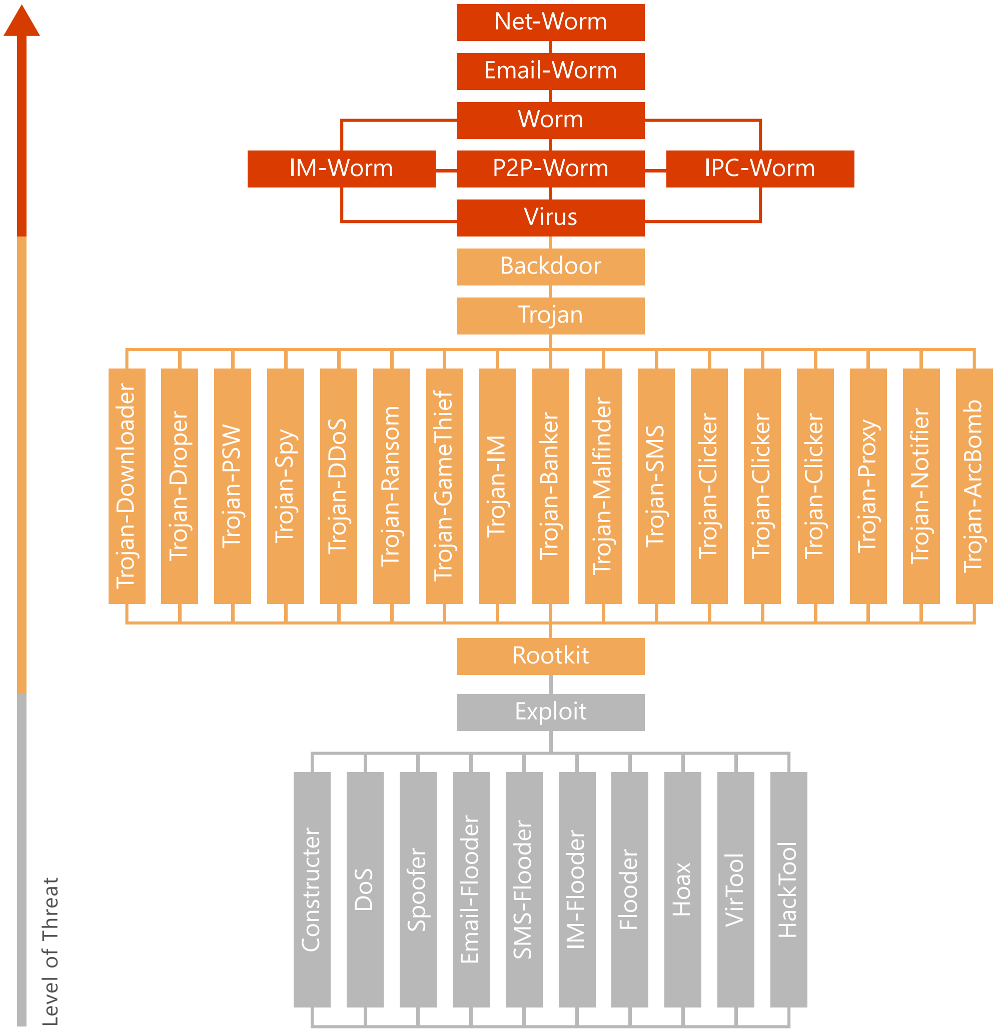


Don’t Be An Easy Target

For security professionals, the message is clear: The best defense is a good offense, and protecting against inbound email threats is essential for business continuity.

Wide-ranging threats exist, with each serving a specific purpose and disrupting users to varying degrees. Some are little more than annoyances, while others require specialized knowledge to detect and remove.

Email Threat Types



“Types of Malware,” 2016, Kaspersky Lab

In addition to email threat types and hacker motivations, understanding attackers' go-to techniques is a big part of a holistic strategy. Attackers gain access to their desired target credentials in four primary ways:

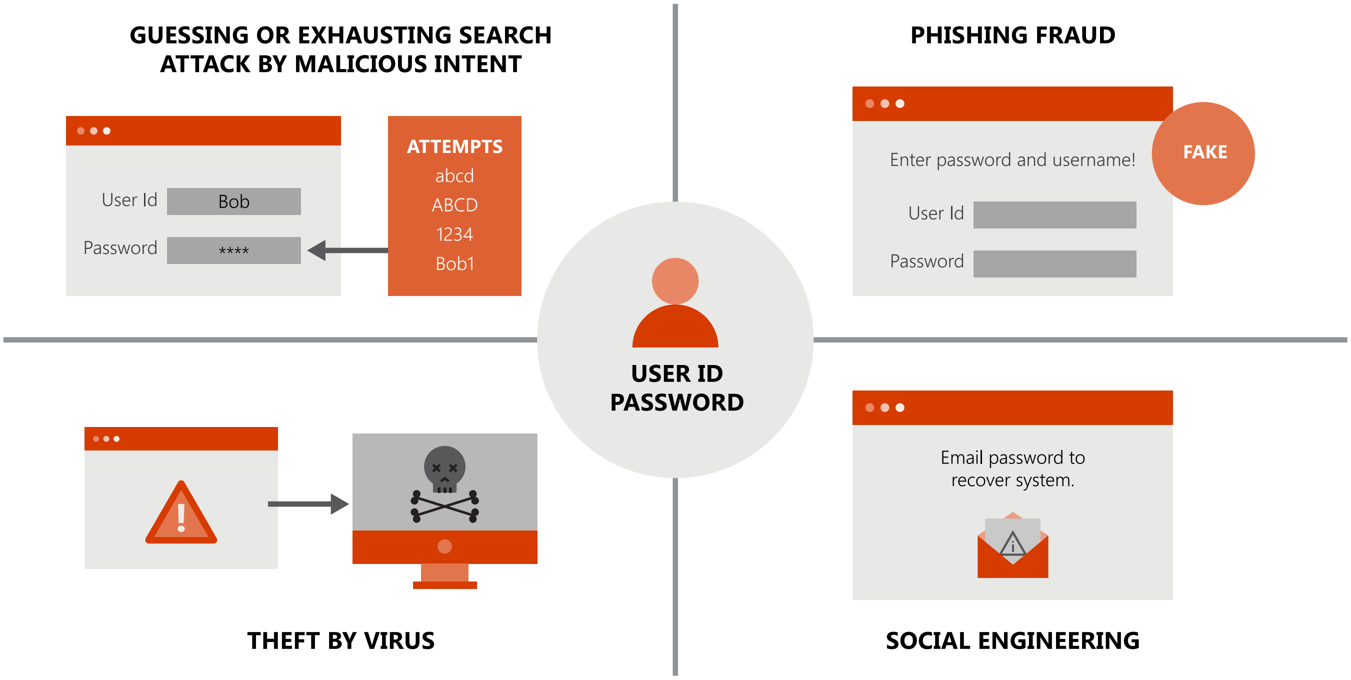
1. GUESSWORK:
Repeatedly trying combinations of usernames and passwords using automated tools and a list of keywords gathered during online research of the target

2. FRAUD:
Using the same list of keywords to compose emails directing the recipient to interact with a well-known financial institution, social network, or vendor by clicking on a link

3. VIRUS ATTACK:
Embedding a virus in an email to gather the required information behind the scenes or grant network access that allows data collection

4. SOCIAL ENGINEERING:
Using a direct request disguised as a trusted contact

Let's look at each of these attack methods in greater detail, highlighting the threat types used in each. Bear in mind that attackers are versatile, typically using a variety of methods and combinations of threat types.



Guesswork

36%

of surveyed respondents work in organizations where IT staff share the same passwords.

"Annual Security Report," 2016, Cisco

Guesswork has little to do with email security, apart from one very important consideration: Email accounts, mail server administrator accounts, and more are secured using usernames and passwords.

Password strength can determine how long it takes an attacker to access an email. Brute force attacks have a single goal: to acquire credentials. Employees need strong passwords as a first line of defense. But according to a Lieberman Software survey, 36% of respondents work in organizations where IT staff share the same passwords, which adds risk of a successful attack. In addition, 55% changed user passwords more frequently than administrative passwords, which is risky, since admin passwords have more system controls and should be changed more regularly than users'.

A 2016 Cisco study notes that 35% of its respondents faced brute force attacks.

Pay careful attention to password strength, as a seemingly innocent email can ask users to supply their login information, which provides an attacker with the necessary data to launch a brute force attack elsewhere in the organization.

Fraud

Email fraud can run the gamut from annoying, non-threatening spam to targeted and non-targeted phishing attacks, but how recipients handle them determines the effects of the attacks. Some users may click on fake invoices presented as email attachments, while others may click on embedded links to sites that then launch a variety of attacks.

Whatever the reason, one of the best ways to reduce the risk of fraud is to train employees so they are aware of common attack methods. They will identify potential attacks more readily and also provide an additional layer of security for the organization. Common attack methods for email fraud include:

PHISHING, SPEAR PHISHING, AND WHALING

To the casual observer, phishing emails are often indistinguishable, leading recipients to a cloned website designed to harvest usernames, passwords, and answers to security questions. Once the information is gathered, the email recipient is then logged into the genuine website, unaware their privacy has been compromised.

Adding another layer of complication, spear phishing's more specific corporate target means that these emails typically appear as internal messages from a trusted company source, such as the IT team.

The highest level of phishing, "whaling," targets a specific person, such as a celebrity, political figure, or business executive. In the business world, this poses an increasingly greater threat to the level of clearance a high-ranking target may accidentally divulge. The emails used to ensnare these potential victims often indicate personal or business knowledge of the recipient, typically gathered after an extensive period of social engineering.

Although phishing attacks are generally decreasing, the ones being implemented are becoming more targeted and complex. In the second quarter of 2016 alone, Kaspersky Lab reported that 8.7% of their total users experienced 32 million phishing attacks (some 2.6 million less than the previous quarter)—occurring more prevalently in China, Brazil, Algeria, and the United Kingdom.

Virus Attack

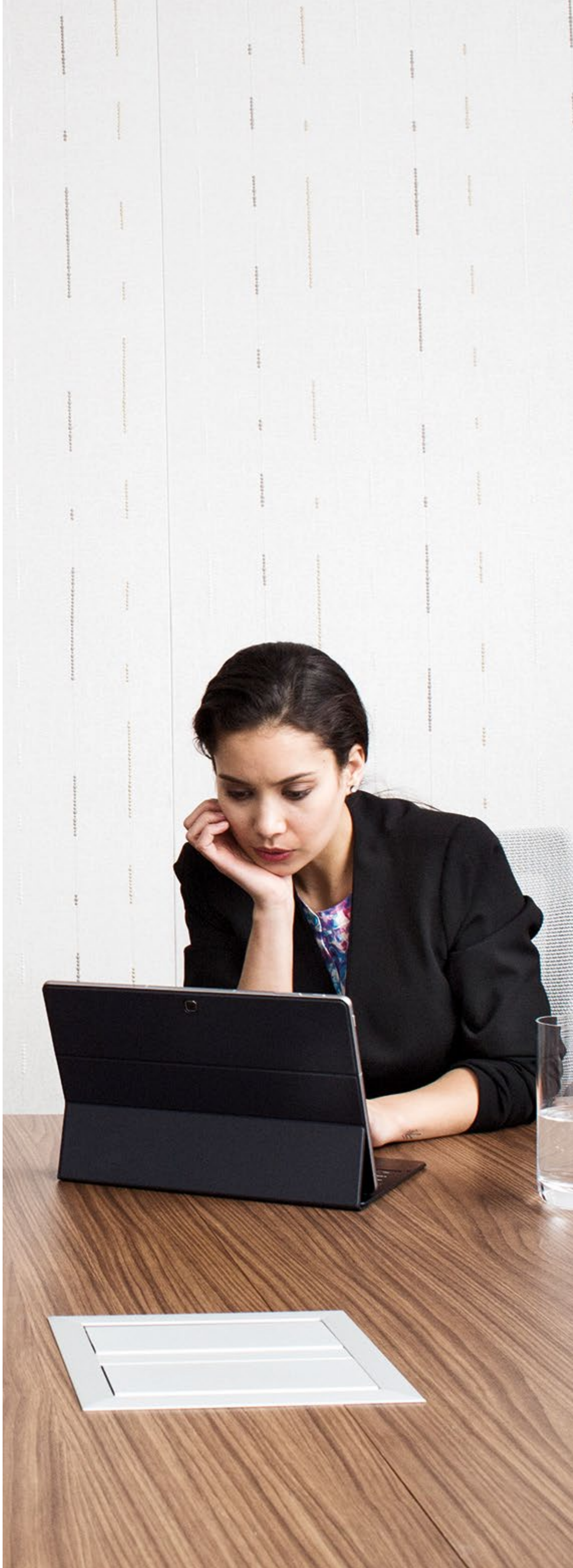
Like a contagious biological virus propagating every computer on your network when files are shared or a particular program is run, computer viruses remain one of the more commonly known forms of attack—usually triggered by clicking on an email attachment or browser pop-up. Some viruses disable the recipient's current anti-virus solution, sending virus-filled emails to everyone in their contact lists. In this manner, viruses can (and have) spread globally in a matter of days.

While an up-to-date anti-virus solution can help, it doesn't always anticipate new viruses that are created every day, relying on software manufacturers to incorporate further removal tools as needed. Virus effects vary widely. Some compromise specific programs, while others render the computer completely useless unless a clean install is performed. Primary attack methods for viruses include:

SPAM

Spam email isn't always just junk. More annoyance than actual virus in itself, spamming still provides an attractive mode of virus delivery. Widespread use of email makes it an ideal vehicle for spammers, who send unsolicited marketing emails to target users, usually without providing an unsubscribe option.

When malicious spammers do slip malware links or attachments into these communications, the results aren't pretty.



SPYWARE

Actively “spying” on its recipients, this form of attack tracks all internet browsing and uses the information to produce ads or obtain clues for later attacks. Recently visited websites, such as banks and retailers, may appear in ads used in later attacks. During a suspected spyware infection, users may notice an altered homepage or experience a reduction in system performance.

One best practice is to review installed programs to see if any are unrecognized and promptly remove any that are confirmed as unnecessary. Removing the suspicious program in question works in many cases to eliminate the source of potential attack; however, resistant spyware will just reinstall itself after reboot. In such cases, use anti-spyware tools to help identify and solve the problem. Occasionally, the spyware may be too complex for automatic removal and require a clean install to help ensure the spyware does not continue to present a threat.

Rootkits, keyloggers, and backdoors also classify as spyware in that they are designed to remain hidden to gather and send information back to an attacker. Given a little time, the attacker is able to collect logins, passwords, financial information, and other private data. Legitimate keyloggers are used to gather corporate computer usage information, but malicious ones operate in the same way, requiring a software install on the target system.

Attackers use a “backdoor” to gain remote access to a network and to install data-collecting malware. With Dipsind, a software program noted in the Microsoft Security Intelligence Report, Volume 20, attackers can quickly design a custom backdoor solution for each target and remain undetected.

Rootkits are one of the hardest types of spyware to detect. Tucked away inside a user- or kernel-level API, they can hide for months and send information to the attacker without your knowledge.

In the first three quarters of 2015, McAfee Labs detected more than 74,000 samples, all from three primary fileless malware families.

ADWARE

Typically considered mostly harmless among computer users, adware's visible function is to display ads on your computer. But some varieties of adware (known as browser hijackers) take over all browser settings, making the computer difficult to use effectively. In such cases, the result can be toxic.

According to AVG, as digital advertising becomes more complex, so does adware. Common adware characteristics include infinite pop-ups, spyware and man-in-the-middle attacks like Superfish, which redirects all your traffic through the attacker's system—even if you're connected to a sensitive site related to online banking.

Disabling certain types of scripts can help, AVG notes, but doing so also impacts the user experience. To remove malicious adware created using the same methods as genuine ads, a dedicated removal tool is often needed.

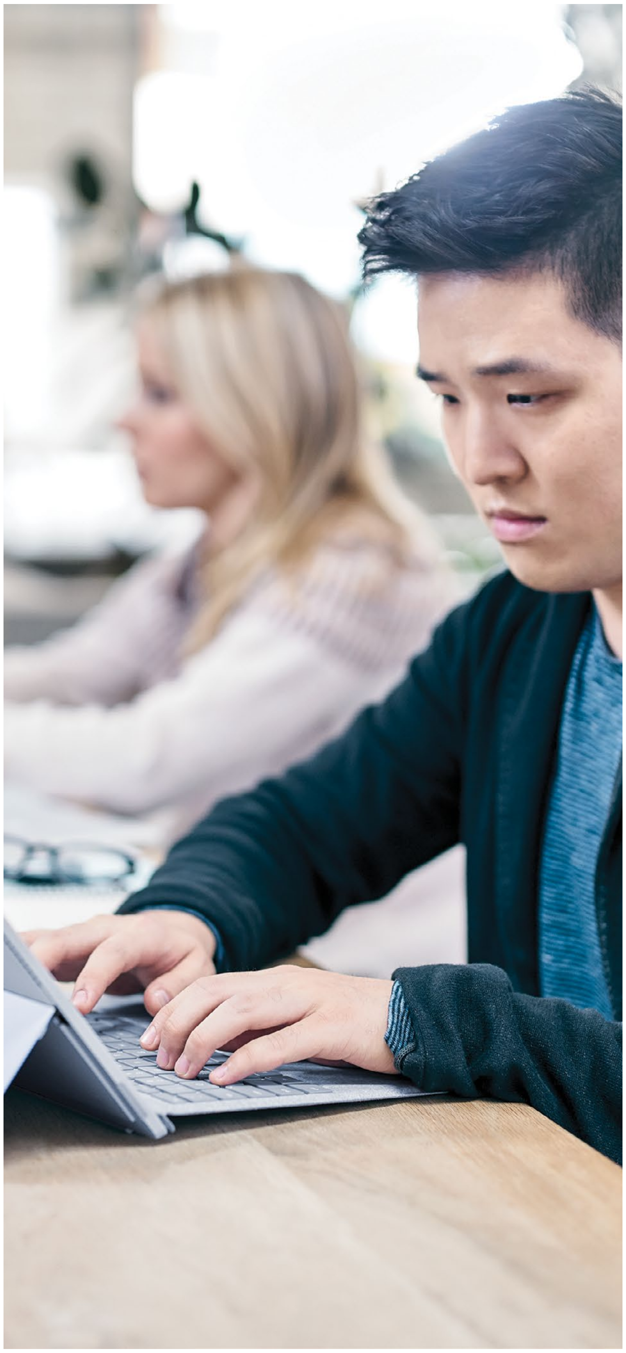
WORMS AND TROJANS

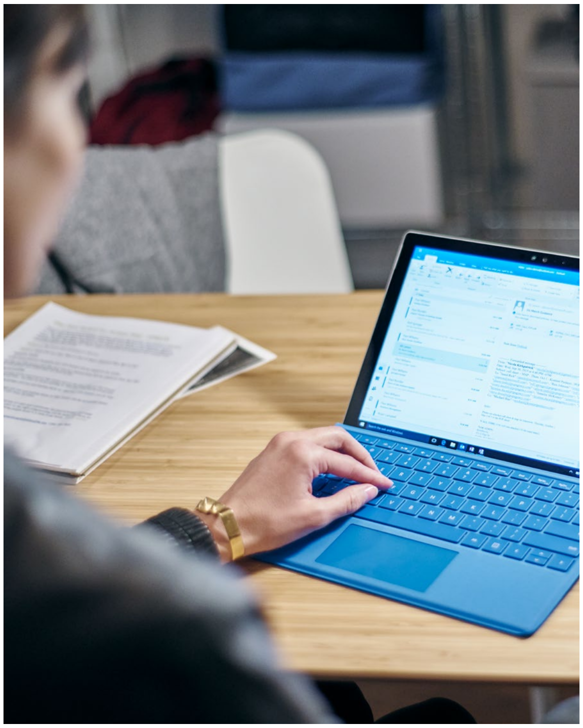
Worms are software programs able to replicate within a computer's system. If left unchecked, they can destroy data until the drive is empty. Most anti-virus programs will detect worms, but new ones can sometimes sneak through.

Considered the most dangerous of all the malware types, Trojans use social engineering to trick users into loading malware onto their systems. Unable to spread on their own, they often have a targeted purpose, such as discovering financial data for later reuse or overwhelming the computer resources entirely, like in the case of a denial-of-service (DoS) or distributed (DDoS) attack.

In 2015, worldwide Trojan-related encounters increased by 57%.

"Security Intelligence Report, Volume 20," 2015, Microsoft





RANSOMWARE

As their name suggests, this type of attack prevents a user from accessing certain apps or programs until a sum of money is paid.

According to Malwarebytes, three distinct ransomware types occur:

Rogue software, known as scareware: A screen prompt appears, informing the user that installation and purchase of software will solve impending system problems. A fake scan lists a wide variety of errors that the software will "fix." Once installed, the remote attacker has not only been paid but can continue to launch other attacks.

Note: Installation of unapproved programs (shadow IT) can allow installation of rogue or fake security programs, disabling existing solutions in the process. Links to such programs are often sent as part of email attachments or invisible links.

Browser- or screen-locking ransomware: A law enforcement warning or similar indication notifies the user to pay a required fine, usually in an untraceable digital currency.

Encrypting ransomware: Not stopping at locking and encrypting all files, this ransomware type also demands payment within a specific deadline before exacting further damage.

20%

of Mimecast's 600 surveyed respondents reported a direct ransomware attack experience.

"Business Email Threat Report," 2016, Mimecast

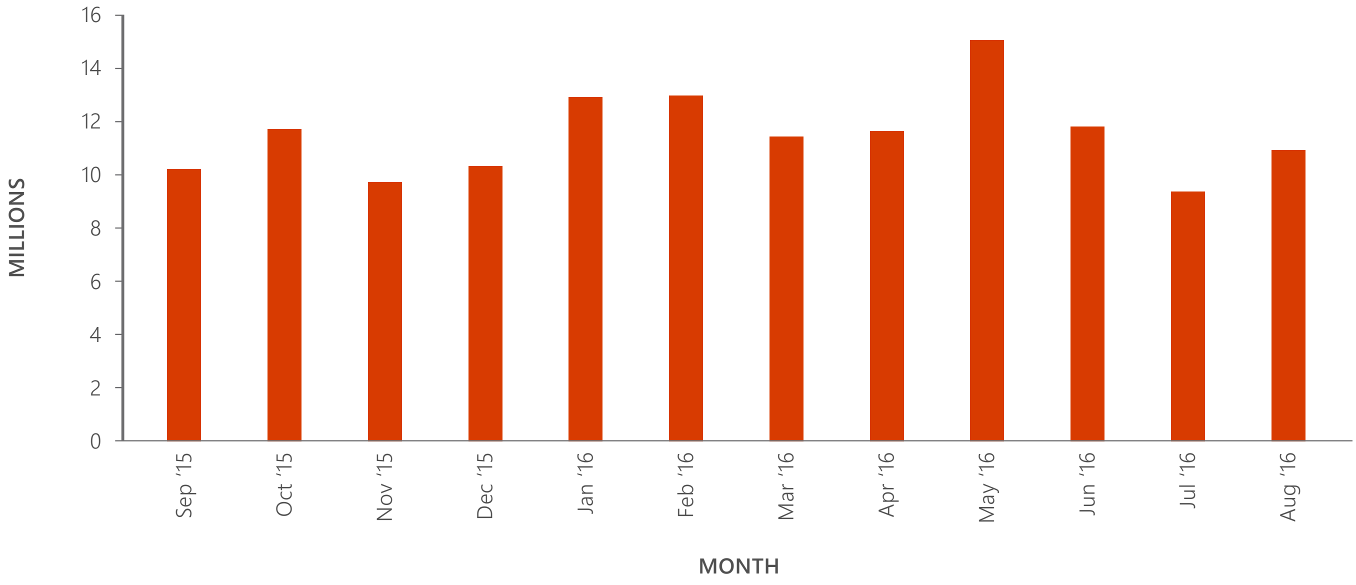
Bypassing the ransom demand screen is difficult, at least until the ransom is paid or you wipe the computer and reinstall everything from scratch. Paying the ransom is an option, but there is no guarantee against other future ransom demands locking up the system.

Unfortunately, ransomware is on the rise. Sophos confirms that email spam is the main delivery method for two of the four primary types: CTBLocker and TorrentLocker. Less-experienced attackers use commercial software exploit kits to deliver the others (CryptoWall and TeslaCrypt) and launch complex attacks.

According to Microsoft, there is no way to fully protect against viruses and malware, but it is possible to reduce infection risks with a combined defense of firewall, updated virus definitions, and adjusted browser settings. Anti-virus software featuring the latest virus definitions is essential to protecting against malware attacks.

Malware Analysis, Sep. 2015–Aug. 2016

"Malware Statistics," 2016, AV-TEST Institute



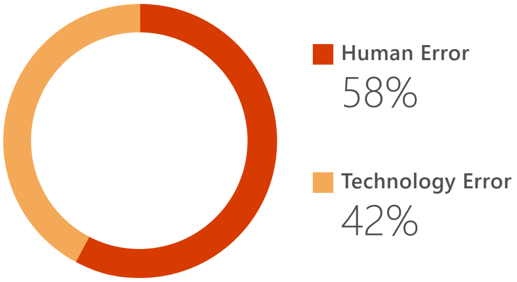
The Human Element

Human error can play a big role in an email security breach, as hackers often rely on an email recipient's mistakes or misunderstandings to successfully attack. Whether it's opening an email or clicking on visible links and attachments, the aim is to encourage the target to let them into the system.

Reducing the likelihood of human error is a key element of any successful email security solution—or indeed any cybersecurity solution. A CompTIA survey confirmed that the primary cause of 58% of security breaches is typically human error, with the remaining 42% related to technology. In those cases, the existing security solution is not enough to block the attack. An effective solution must reduce human error and be sophisticated enough to solve technological problems—all while protecting against primary email attack methods spanning spam, phishing, malware, or new attack vectors.

Primary Cause of Security Breach

"International Trends in Cybersecurity," 2016, CompTIA



Although most companies employ hardware or software technology solutions to combat a variety of internal and external security threats, problems caused by human error remain difficult to solve. According to SANS, most enterprises have employee security awareness programs in place, but three primary deficiencies often hamper their efforts: lack of technical and financial resources, management support, or staff training.

Consider the impact of human error on each of the inbound threats discussed in this section. What makes them successful? In almost all cases, these virus types employ an email delivery method as part of an initial attack. Recipients open emails from unknown parties and click on links or attachments. How can this problem be solved? Bearing in mind that each received email can have several attack functions, a strong way to approach security threats is from the mindset of the attacker. In other words: Know your enemies and their methods of attack.

SOCIAL ENGINEERING

It takes many forms, but social engineering plays a major role in inbound email threats. Whether the potential threat is based on spam, attachments, or links, IT must consider users as a primary soft spot in a company's security perimeter and act accordingly. Attackers will use a variety of methods to gain network access or user credentials. They will mix and match viruses where appropriate and can customize these viruses to create new undetectable strains. Therefore, security awareness and vigilance are key in reducing human error on the recipient's end. Employee training and protocol for avoiding suspicious contact and raising IT concern is paramount.

PERSONAL USAGE

With many employees using corporate email accounts for personal use, receiving emails from a personal contact with an infected computer introduces additional risk. Employees are certainly more likely to open an email from a trusted contact, which increases the risk of infection given that consumer computers lack enterprise-class solutions to block common threats.

According to an Alfresco survey, more than half (51%) of business professionals use personal email for work-related tasks, and only 38% think of data security when collaborating externally.

In the interest of data and network security, one best practice is to advise users to segregate business and personal emails. They should use personal accounts for activities without a business focus.

A Holistic Security Approach

To anticipate these primary attack methods, an effective email security solution should cover several bases, including but not limited to:

- Reducing human error by taking a proactive approach to email processing and employee education
- Automating the manual screening of incoming emails
- Verifying sender, links, and attachments before email reaches the intended recipient
- Separating problematic emails for confirmation and eventual deletion
- Quickly sending all verified emails, with clean links and attachments, to their intended recipients

Delayed email traffic is not an option for any business, so the entire process needs to be fast and accurate. Doing so requires a combination of big data, real-time threat intelligence, and machine learning to ascertain each user's email usage and patterns on an ongoing basis. It must also operate seamlessly with products from other security vendors, while offering a cost-effective per-user cost.

With incoming emails' contents containing any amount of sensitive details on pending contracts, mergers, litigation, or other confidential information, security remains of paramount importance. Opening up data to a third party gives attackers an additional target and increases the risk of data loss. Limit the risk of data loss by utilizing a single email security solution, without outsourcing any of the process stages to third parties.

An effective email security solution works to protect, detect, and respond:

Protect across all endpoints, from sensors to datacenter.

Detect using targeted signals, behavioral monitoring, and machine learning.

Respond by closing the gap between discovery and action.

Internal Threats

With so many outside threats to your company's data, it can be easy to overlook those internally as well. To cover all concerns, organizations must still consider outbound email's potential for data loss and factor it into their email security strategy.

In fact, the IT professionals surveyed in Mimecast's report reveal that malicious insider attacks rank as their top perceived company vulnerability—even above malware, phishing, and social engineering.

As a result, 69% of IT security professionals who noted having experienced email hacks now also have data leak prevention and other internal threat mitigation protocols in place.

The following pages outline the types of internal email threats that can generate security risks within your organization and what you can do to avoid them.

Malicious Insider Attacks

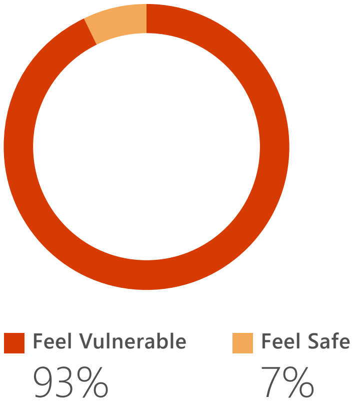
Perhaps the most difficult internal threat to handle, malicious insider attacks can be particularly damaging. Although there are other ways to send confidential data outside the company (such as memory sticks, cameras, and more), email remains a convenient means for malicious insider havoc.

Organizations are on the alert but not always sure how to proceed. A 2015 Vormetric Data Security report shows that 93% of organizations in the United States feel vulnerable to insider attacks.

With an established Data Loss Prevention (DLP) policy, organizations can proactively protect confidential data—tracking, blocking, or allowing the transmission of sensitive data on a per-user basis. This functionality is based on a combination of user permissions and prior classification of sensitive data types.

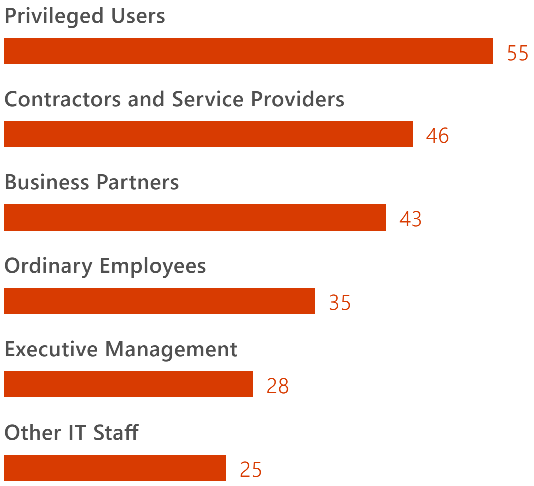
U.S. Company Perception of Insider Attacks

"Insider Threat Report," 2015, Vormetric Data Security



Employees Who Pose the Largest Risk of Insider Threat

Percentages by User Group



"Insider Threat Report," 2015, Vormetric Data Security

Accidental Confidentiality Breaches

Sending an email to the wrong recipient is embarrassing, but if it also includes proprietary or confidential company data and correspondence, the temporary discomfort is insignificant compared to the potential for irreparable business damage.

Whether it is intellectual property (IP), documented internal processes and procedures, business plans, or client data, company information must be protected at all times to prevent users from sharing business-critical or confidential data by email.

Depending on the organization's industry and activities, the loss of data doesn't just cause reputational damage; it can also lead to heavy fines and penalties from governing bodies for non-compliance.

The cost of data breach varies by industry and the sensitivity of the information leaked, but a 2015 Ponemon Institute study shows that human error typically costs the employee's company about $117 per breach.

Whether accidental or deliberate, human error is a genuine security risk. A comprehensive email security solution can implement security checks to prevent users from sharing confidential information over email, either by providing warnings or notifying administration.

The Ponemon Institute reports that 47% of global data breach incidents involve a malicious or criminal attack, versus 25% stemming from a negligent employee or contractor.

"Cost of Data Breach Study: Global Analysis," 2015, The Ponemon Institute

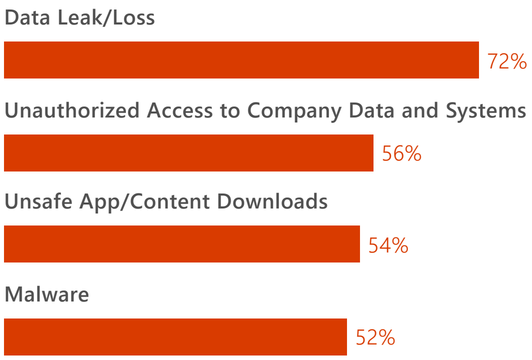
Risks Associated With Connected Devices

The rise of bring-your-own-device (BYOD) programs and use of connected mobile devices throughout organizations has increased productivity, enhanced collaboration, and allowed users to have immediate access to email—regardless of their physical location.

With all these benefits, however, comes a fair share of risk. The fact that email is accessible from so many connected devices means that it must be part of any effective email security solution, as these devices are subject to the same inbound and outbound threats as their desktop counterparts.

Companies' Main BYOD Concerns

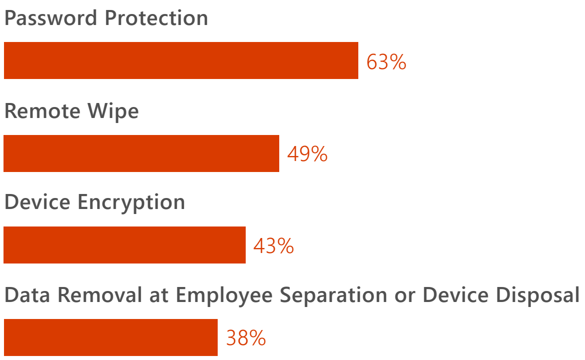
"Spotlight Report: BYOD and Mobile Security," 2016, Information Security



Create a BYOD policy that prepares for eventualities such as loss or theft of a mobile device (a remote wipe facility to erase data, for example). It should have clearly defined data retention policies and include provisions for when employees leave the company.

Most Common Measures for BYOD Risk Control

"Spotlight Report: BYOD and Mobile Security," 2016, Information Security



If an employee leaves the company with his or her personal mobile device, all company data (including email and instant messaging) should be securely removed from that device. The data on the device, however, must be moved and retained on company servers in case of litigation or to satisfy other compliance requirements.

The ideal email security solution should be platform-independent, working equally well across PCs, tablets, and smartphones.

Legal Compliance Factors

All organizations have a variety of compliance factors to consider, notably related to storage, privacy, and security of data—all of which can be compromised if email security is below par. Some standards are legislative and based on jurisdiction, data privacy, and data governance laws, for example, while others are industry-specific and are required to do business.

Data retention requirements are yet another consideration. In terms of outbound email storage, the data retention period varies depending on the jurisdiction or standard, but five years is typically considered the absolute minimum for business accounting. This section covers common compliance instances organizations must watch for and how to proactively keep them in mind.

MEETING INDUSTRY STANDARDS

Some industries' regulations, compliance, and standards are more complex than others'. Managing these standards can be overwhelming and time consuming, and many require a third-party organization to verify a company has fulfilled its obligations. Some are also mandatory, while others demonstrate industry expertise or compliance with a specific set of quality standards.

This gives organizations a range of reasons for ensuring compliance to a given standard—chief among them include reducing liability, enhancing company reputation, satisfying shareholders' interest in company progression, and reducing costs. These costs can range from customer compensation to litigation to non-compliance fines from regulators.

The most challenging aspects of compliance, however, lie in two primary but connected areas: data loss and data privacy. Data loss is immediately obvious, whereas data privacy can be more difficult to pinpoint—referring in many jurisdictions, including the United States, to personally identifiable information (PII).

A key feature common to many standards is confidential data management. Data loss can occur through outbound emails, posing critical security risks that could lead to non-compliance and corresponding penalties. Regulatory violations can also occur when client or patient information is sent to the wrong receiver, whether externally or within the company.

How can organizations proactively approach their legal compliance challenges? Here are critical industry standards to consider:

PROTECT CARDHOLDER INFORMATION WITH PCI-DSS

Companies that offer to accept credit card payments must comply with the Payment Card Industry Data Security Standard (PCI-DSS). Protecting cardholder information is just one control objective defined in the standard, along with maintaining strong access control measures and an information security policy.

Failing to meet compliance standards can result in fines, penalties, and loss of credit card processing capabilities—not to mention a damaged reputation.

80%

of businesses failed their interim compliance assessments for meeting PCI security standards, according to a 2015 Verizon report, which increases their risk for data breaches and financial and reputational damages.

PROTECT PATIENT INFORMATION WITH HIPAA (HEALTH CARE)

Organizations in the United States health care industry must protect patient information confidentiality and are expected to comply with the Health Insurance Portability and Accountability Act (HIPAA). Information security breaches are of utmost concern, with varied consequences for non-compliance including fines, civil and criminal penalties, and increased scrutiny if data loss occurs.

Other countries have different standards to achieve the same goal, but all with a common aim to protect digital health records and ensure that health care organizations are capable of prudently managing patients' information.

PCI compliance violations can result in $5,000–$100,000 per month.

"PCI Compliance Report," 2015, Verizon Enterprise

With 4 categories of violation based on level of negligence, penalties can run up to $1.5 million per violation, per category, per year.

"What are the penalties for HIPAA violations?" 2015, HIPAA Journal

ADHERE TO THE SECURITY STANDARDS OF FISMA (FEDERAL)

To maintain high-level security at the national level, the Federal Information Security Modernization Act (FISMA) outlines required compliance elements across all United States federal government agencies, their contractors, and other organizations that work on their behalf.

Failure to comply introduces security vulnerabilities that could enable attackers to exploit and obtain valuable federal data or attack key infrastructures such as power generation and city planning. Along with reputational damage, penalties for non-compliance also include congressional censure and loss or reduction of federal funding.

EDISCOVERY CHALLENGES

Managing email as part of an ongoing data management strategy is a complex task that is impossible to achieve manually. It's particularly challenging when emails are requested as part of a civil or criminal litigation, known as "electronic discovery" or eDiscovery. Companies must produce evidence of specific emails, who received them, and how they were dispersed. Organizing this data proves difficult, as the information must be presented in court in a human-readable format. Additionally, increased technological mobility caused by mobile devices and BYOD can create another layer of complexity.

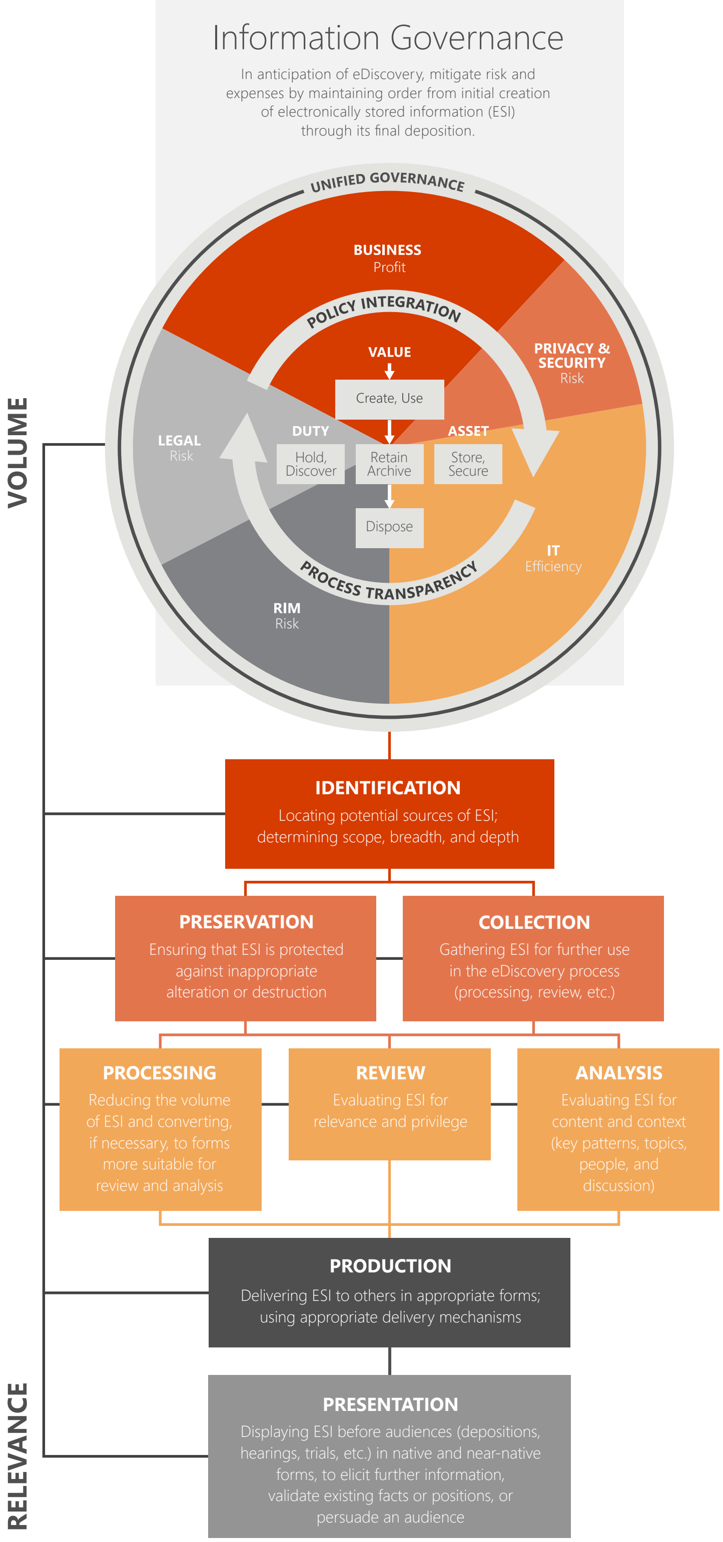
How can an organization know exactly from which devices the email was disseminated? Can the organization track all messages (including replies and forwards) on all devices that relate to that single original email? This is where many organizations have difficulty.

A platform designed specifically to handle email for eDiscovery takes the task from daunting to doable, automating much of the necessary requirements and reducing the time and expense traditionally spent on these activities. Machine learning is particularly useful, providing the ability to easily extract and visualize required data based on user-defined queries as well as evolving algorithms generated according to usage and storage patterns.

With an eDiscovery tool linked to your entire business suite, including email, these features can help you with auditing or following compliance.

Electronic Discovery Reference Model

Standards, Guidelines and Practical Resources for Legal Professionals and eDiscovery Practitioners


Information Governance
In anticipation of eDiscovery, mitigate risk and expenses by maintaining order from initial creation of electronically stored information (ESI) through its final deposition.
UNIFIED GOVERNANCE
BUSINESS
Profit
POLICY INTEGRATION
VALUE
Create, Use
PRIVACY & SECURITY
Risk
LEGAL
Risk
DUTY
Hold, Discover
Retain Archive
ASSET
Store, Secure
Dispose
IT
Efficiency
PROCESS TRANSPARENCY
RIM
Risk
VOLUME
IDENTIFICATION
Locating potential sources of ESI; determining scope, breadth, and depth
PRESERVATION
Ensuring that ESI is protected against inappropriate alteration or destruction
COLLECTION
Gathering ESI for further use in the eDiscovery process (processing, review, etc.)
PROCESSING
Reducing the volume of ESI and converting, if necessary, to forms more suitable for review and analysis
REVIEW
Evaluating ESI for relevance and privilege
ANALYSIS
Evaluating ESI for content and context (key patterns, topics, people, and discussion)
PRODUCTION
Delivering ESI to others in appropriate forms; using appropriate delivery mechanisms
PRESENTATION
Displaying ESI before audiences (depositions, hearings, trials, etc.) in native and near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience
RELEVANCE

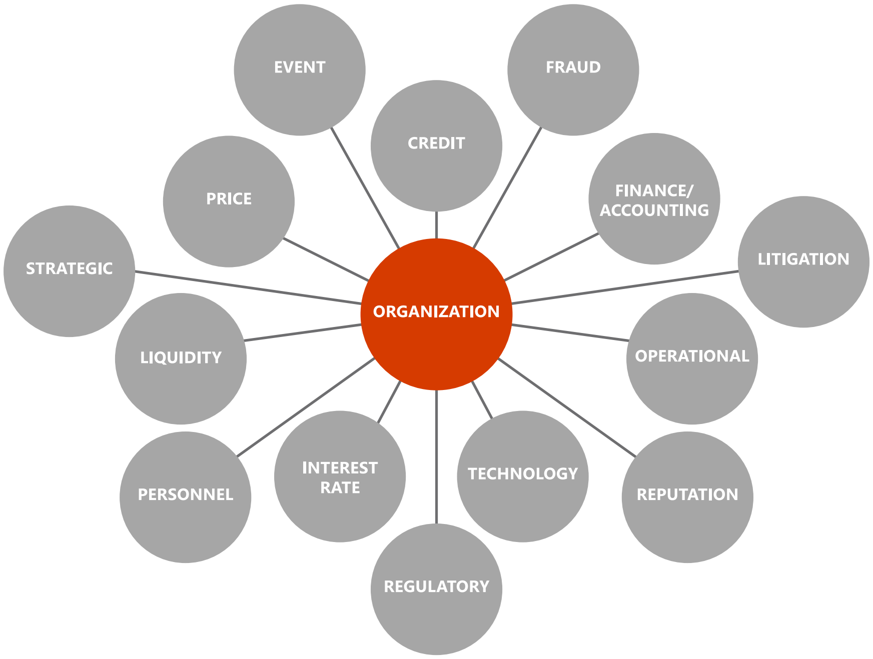
The Ideal Email Security Solution

By taking a more detailed look at internal threats, you can further define the ideal email security solution needed for your business.

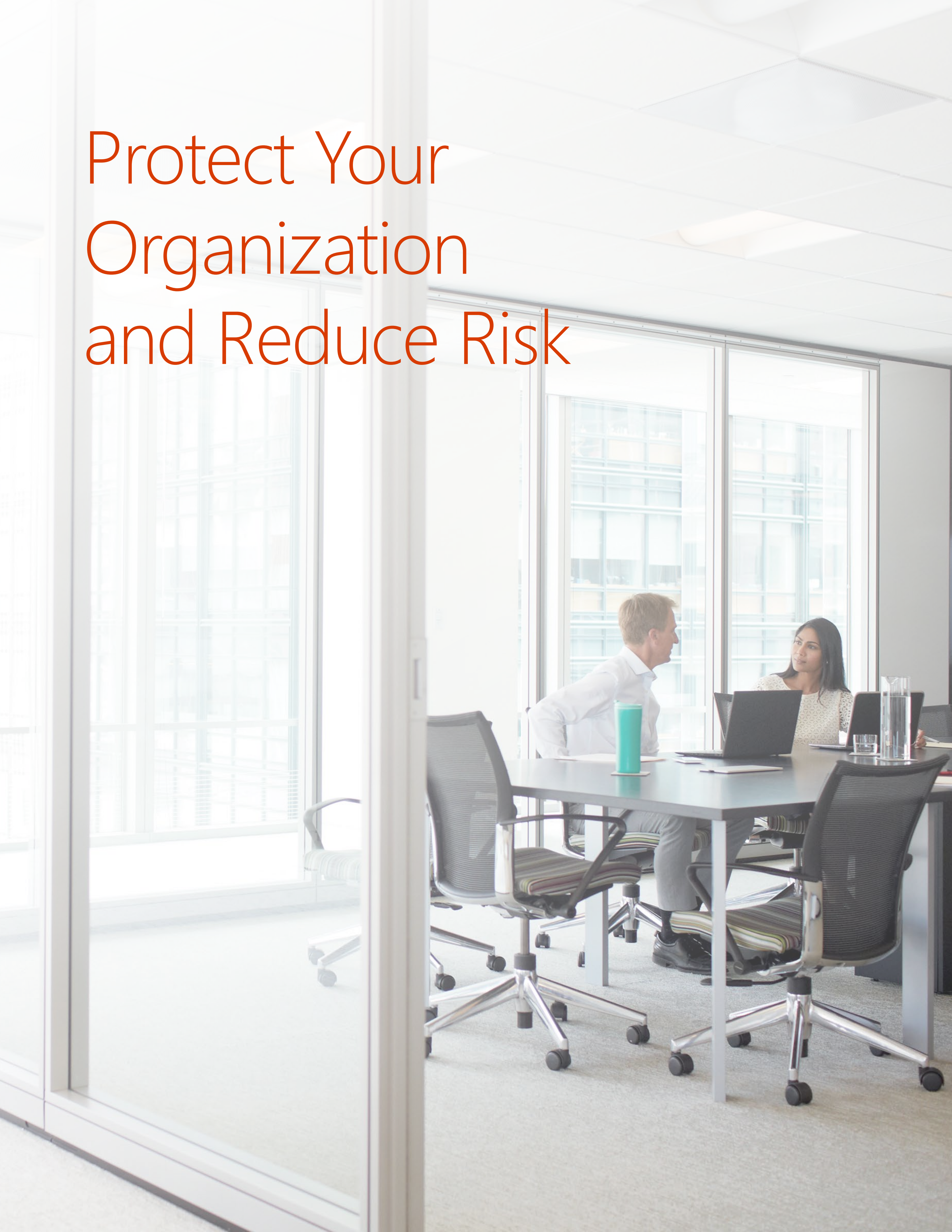
- Automate screening on all outbound emails to help prevent data loss, proactively seeking to eliminate human error.
- Protect confidential data by classifying documents and other information as sensitive where appropriate.
- Require user authentication permissions for sending sensitive data.
- Send prompts alerting users to acknowledge when an outgoing message contains sensitive data.
- Promptly deliver outgoing email to ensure time sensitivity.
- Handle regulations, compliance, and eDiscovery needs—regardless of platform or device.

Whether the data is from the company, an employee, a partner, or a client, IT needs a strategy in place to help protect it all.

Enterprise Risk within a Typical Organization



Protect Your Organization and Reduce Risk



The prevalence of cloud services has changed how many organizations structure their IT, with many turning to third-party solutions for support. A recent IDG Connect survey indicates that hybrid IT (a mix of cloud and on-premises IT) is becoming more widely accepted, with 80% of respondents planning adoption in 2016.

Selecting a cloud service provider, however, requires trust that the service storing and managing your data is compliant with relevant laws, regulations, and industry standards to keep your business on track. As an end-to-end security specialist for more than 20 years, Microsoft knows the key role your data plays in your company's success.

Although no security solution can offer 100% protection from attackers, you can find one that helps meet your privacy, transparency, security, and compliance needs. With the latest versions of software, your company can stay up to date with the most current security insights available.

Office 365 Protection Principles:

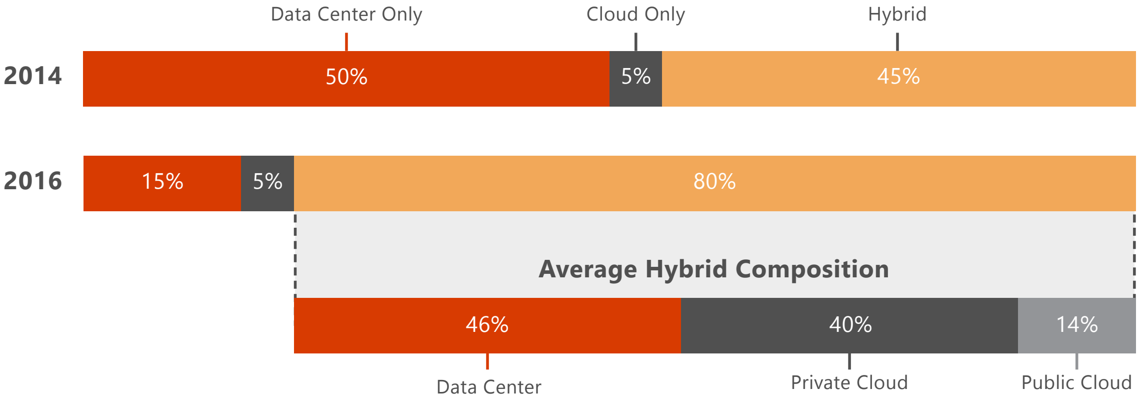
Pervasive: Office 365 has built-in data protection features that provide a high degree of confidence in the cloud.

People-Centric: Office 365 is built around how people work, to increase security and compliance without getting in the way of employee productivity.

Intelligence: Office 365 is smart on your behalf, providing visibility into risk and suggesting solutions to limit exposure.

Usage of Computing Models

By Percentage of Respondents



"The Rise of Hybrid IT," 2015, Interxion/IDG Connect

Security You Can Trust

Microsoft's long-time track record for providing next-level security features strengthens IT team security management. Office 365 users enjoy an email solution with comprehensive security features that help mitigate risks of data breaches and industry-related legal non-compliance.

Designed with compliance in mind (ISO 27001/27018, PCI DSS, HIPAA, FISMA, FedRAMP, EU Model clauses, GLBA, and many more industry standards), Office 365 helps you meet your obligations. Microsoft achieves these standards in order to help match or exceed the requirements necessary, with each standard requiring third-party verification audits to achieve certification.

SERVICE-LEVEL SECURITY

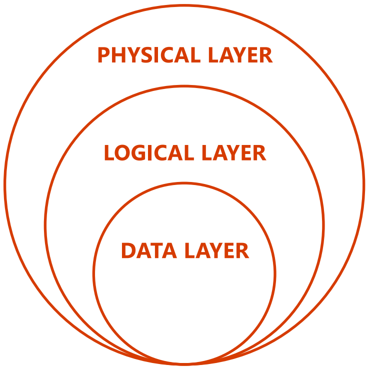
Physical, logical, and data layers in Office 365 provide security controls to help protect against data breaches in various forms and provide backup protection should a breach occur. This in-depth defense strategy also includes tactics to detect, prevent, and mitigate security breaches and to continually provide system improvements, such as:

- Port and perimeter vulnerability scanning
- Operating system security updates
- Network-level distributed denial-of-service detection and prevention
- Multi-factor authentication for user/service access

In addition, internal precautionary measures include regular audits of operator/administrator access and actions, employee email segregation and analysis, and mandatory background checks for privileged access.

1. THE PHYSICAL LAYER (ON-PREMISES ACCESS)

Security at the physical layer is essential. All Office 365 datacenters are created with the same attention to security and privacy, to provide protection at the site of data storage as well as on the web.



Onsite access to the datacenter requires multiple authentication processes, including biometrics, smart cards, and two-factor authentication. Onsite security guards, video surveillance, and motion sensors provide additional protection to prevent nonessential personnel from gaining access to facilities.

Automated fire prevention and extinguishing systems provide protection from natural disasters, and racks are braced for seismic activity in locations where necessary.

At a network level, only the connections and protocols necessary for service operation are allowed. All other connections are blocked to compartmentalize data, with edge routers to detect intrusions and signs of vulnerability.

2. THE LOGICAL LAYER

In the logical layer, host and application processes and controls are automated as much as possible to reduce human error, malicious or otherwise. Administrators maintain strict control by allowing only the amount of access required to complete specific operations.

Whether it's anti-malware updates, patches, configuration management, or related tasks, all are verified before implementation and follow a defined change management process with audit controls.

3. THE DATA LAYER

While customers may share hardware resources, Microsoft employs data isolation techniques that help ensure data privacy. This is achieved by segregating each tenant in Azure Active Directory, thereby preventing one tenant from accessing another's data. In addition to multi-layer protection of the service, Office 365 also offers additional protection from threats.

Threat Protection

Using an "assume breach" strategy (by making the assumption that a breach has already occurred), Office 365 is designed to force continuous improvement to its built-in security features. This is achieved using a four-pillar approach of prevention, detection, response, and recovery.

Prevention includes the layered techniques used to protect the datacenters and all the measures taken to stop breaches before they happen.

Detection uses machine learning and collects all system and security alerts, combining them with external signals and eliminating false positives before triggering system alerts.

Responses are developed to mitigate the effects should breaches occur. Processes are put in place to detect incidents in a timely manner and block access to data or servers as quickly as possible to reduce data loss.

Recovery encompasses the procedures necessary to return to standard operations and includes changing security principals, auto-updating affected systems, and auditing the system.

Office 365 provides security features that can be difficult for organizations to achieve on their own. It uses machine learning, big data, and more to maximize threat intelligence and reduce security risk, enabling IT teams to use their time on initiatives that drive business forward.

Your business continuity is on the line. Microsoft's Office 365 cloud-based subscription service gives organizations instant access to the latest versions of all the core Microsoft Office applications, as well as Skype for Business, OneDrive for Business, and Exchange Online. As email attacks become more complex, Office 365 takes a comprehensive approach that can help fill gaps in security that often otherwise require multiple vendor solutions. While still designed to integrate with other security vendors' products when necessary, Office 365 helps safeguard corporate data and defend your organization against cybercrime.

Looking for an email security solution that provides powerful protection against threats, compliance risks, data loss, and more? Take a self-guided tour of the entire suite to find out how Office 365 can help protect your organization.

Sources

"Business Email Threat Report," 2016, Mimecast

"Quarterly Threat Summary," 2016, Proofpoint

"Data Breach Investigations Report" 2016, Verizon

"Flipping the Economics of Attacks," 2016, The Ponemon Institute

"Types of Malware," 2016, Kaspersky Lab

"RSA Conference Cyber Security Survey," 2016, Lieberman Software Corporation

"Prevent Identity Compromise," 2016, Microsoft

"Annual Security Report," 2016, Cisco

"Spam and Phishing in Q2 2016," Kaspersky Lab

"Security Intelligence Report, Volume 20," 2015, Microsoft

"Threats Report," 2015, McAfee Labs

"What is Adware and How do I Get Rid of It?" 2015, AVG Technologies

"How to Protect Your Business From Ransomware," 2016, Malwarebytes

"The Current State of Ransomware," 2015, Sophos

"Guard Your Business Against Viruses, Spyware, and Malware," 2015, Microsoft

"Malware Statistics," 2016, AV-Test Institute

"International Trends in Cybersecurity," 2016, CompTIA

"Security Awareness Report - Securing The Human," 2016, SANS Institute

"Collaboration Trends and Technology: A Survey of Knowledge Workers," 2015, Alfresco/Dimensional Research

"Insider Threat Report: Trends and Future Directions in Data Security (Global Edition)," 2015, Vormetric Data Security

"Cost of a Data Breach Study: Global Analysis," 2015, The Ponemon Institute

"Spotlight Report: BYOD and Mobile Security," 2016, Information Security

"PCI DSS Quick Reference Guide," 2010, PCI Security Standards Council

"PCI Compliance Report," 2015, Verizon Enterprise

"What are the Penalties for HIPAA Violations?" 2015, HIPAA Journal

"Federal Information Security Modernization Act (FISMA)," 2016, Homeland Security

"The Rise of Hybrid IT," 2015, Interxion/IDG Connect

"Office 365: Security and Compliance," 2016, Microsoft