clearswift
by HelpSystems

2019 Cyber Etiquette:

A Guide To Today's Top Cyber Threats

“Gaining a clear understanding of today’s cyber threats enables you to put the right measures in place to mitigate them.”

***Dr. Guy Bunker**, Chief Technology Officer, Clearswift*

In today’s world of digital collaboration, IT security has become one of the most important areas that organizations – both large and small – must consider as part of their business strategy in order to protect their operation from cyber-attacks and data breaches. Subsequently, IT Security teams and suppliers are under immense pressure to keep up with the evolving threatscape and ensure the right technology and processes are in place to effectively prevent cyber threats striking an organization.

Our ‘2019 Cyber Etiquette: A Guide To Today’s Top Cyber Threats’ is an educational piece designed to help readers better understand the cyber threats that organizations across the globe are facing as we collaborate online for business. It includes descriptions of threats, what to look out for, proactive prevention approaches and technology tips to take away and deploy at an organization.

Prevent Threats. Protect Critical Information. Comply with Regulations.

Contents

#1 GDPR:
Data protection just got serious

What is it?

The General Data Protection Regulation (GDPR), which came into effect on 25th May 2018, is a legal framework that sets guidelines for the collection and processing of personal data within the European Union (EU). The new regulation is a welcome change to data privacy that aims to give control to citizens over their personal data and to simplify the regulatory environment for businesses, including those outside of the EU. Compliance with GDPR is now an on-going consideration for organizations across the globe which shouldn't impact the day-to-day running of a business. However if a company is not prepared, it can damage the business.

Why is it a threat?

Being stung by GDPR does not depend on a targeted attack or malware issue, it also relates to data breaches from within, including the business supply chain. If a business holds and processes EU citizen data and does not comply with the GDPR, the fines can be crippling – either €20 million or 4% of the organization's turnover, whichever is the higher figure, so not an insignificant sum.

In addition to the threat of fines for non-compliance, there is also the potential to weaponize GDPR. This threat can be executed by traditional cybercriminals, hacktivists (who are socially or politically motivated) or disgruntled customers and employees. To achieve their goal, an attacker will target an aspect of the organization they believe to be in violation of GDPR in order to get the business fined or damage their reputation. They could also be looking to grind the business to a halt, something they can achieve by inundating the organization with 'right to be forgotten' (RTBF) requests.

3 things for businesses to watch out for

1. Consent

Consent, or rather a lack of, is the easiest way for attackers to go after a company to cause damage. Ensure that all sensitive data your organization holds and processes is with consent from the customer.

2. Right to be forgotten (RTBF)

Completing a RTBF request will be the biggest drain on a company's compliance resources and being unable to successful complete a RTBF request could result in a major fine and potentially the company grinding to a standstill. While an organization has a month to complete the request, it's important to ensure there is a process in place to recognize and address these requests as soon as possible.

3. Shared responsibility

The shared responsibility clause within GDPR also means a company is responsible for the data shared across the entire information supply chain. This means that if a partner does not have adequate data security measures in place and a data breach occurs, both companies will be held accountable. Ensuring all companies in the information supply chain have the same level of security is a must.

A holistic approach to securing your business against this threat

People

Employees need to be educated about the consequences of non-compliance for the company as well as their own responsibilities when handling sensitive data. Alongside this, they will need to know what processes to follow when it comes to reporting a GDPR issue. This includes making all employees aware of how they can help increase security, including best practices and good data citizenship.

Process

It's now crucial to have processes in place around what to do should a RTBF request come in and how to handle sensitive data. However, it's also vital to have processes in place for if (or when) something goes wrong. Employees need to know if there's a compromise or personal data is lost, such as who to report to internally and how to report the incident to those affected.

Technology

Technology can be used as a line of defense as well as to enforce an organization's policies and processes. A next generation **Adaptive Data Loss Prevention (A-DLP)** solution will help mitigate sensitive data loss risks through an organization's digital collaboration channels. It also has the ability to protect an organization from someone sending sensitive information in error – before it leaves or enters the network. The latest email and web security solutions include **Sanitization** and **Data Redaction** features which work together with a deep content inspection engine to detect and redact sensitive data within emails and attachments, including metadata, before its received in an Inbox or uploaded to the web. **Encryption** is another powerful tool that can be used to enhance secure information sharing across email. In addition, ensure you have a process in place to be able to find personal data quickly and efficiently within your various business systems so you can effectively execute a "right to be forgotten" request.

Cyber Etiquette Guide

- It's not just the IT department that has to worry about data protection. GDPR affects all affects all employees' way of working and so ensuring you have a clear idea of how to handle sensitive data is key.
- Shared responsibility means everyone. When handling personal data, remember that you will be held accountable should you cause a compliance issue. Before sending an email or document, think twice about what information is there and who it's going to.
- That email could be malicious. Look out for traditional signs of phishing emails (such as unusual email addresses or requests for bank details) as these can steal data and cause a major compliance issue.
- If you're not sure, ask. There are a number of clauses with GDPR which you might not think apply to you. It's always worth checking in with either the designated GDPR officer or the IT department to get clarity on anything you're unsure of. It's better to be over-prepared than under-prepared.
- Connecting devices. Non-compliance with GDPR can be caused by simply by plugging in a USB stick and transferring data onto the device. Make sure if you are using a storage device, you encrypt the USB or files so the data cannot be stolen.

#2 PHISHING: Don't take the bait

What is it?

Phishing gets its name from its closely related homophone and much like fishing, it uses bait to catch a victim. Phishing is the attempt to obtain sensitive information, such as email addresses, passwords or bank details, via disguised emails from malicious senders. A victim of a phishing attack is someone who receives an email appearing to be from a trusted sender (for example, someone who emails you frequently) which has an infected attachment or link. The infected link goes on to download malware onto the victim's PC which then goes on to steal personal information from the individual or company.

Why is it a threat?

Phishing scams are dangerous because they are not always noticeable. An email that looks to be something you would receive as normal could actually be hiding malware that is activated once you've clicked on the link. When the malware is activated, the cybercriminal then has access to sensitive data which can be stolen and leaked, leaving the company in hot water when it comes to GDPR compliance.

It's vital to remember that all information has a value to somebody and that's what makes phishing scams so dangerous. Even information that seems insignificant to your organization can be used maliciously, whether that is to weaponize GDPR – by making it impossible to complete right to erasure requests – or to provide a competitor with invaluable information.

3 things for businesses to watch out for

1. Whaling

This kind of phishing attack targets top level executives. Cybercriminals will specifically target C-level employees with emails that appear to be safe and from a trusted source, in order to install malware onto the individual's device and gain access to sensitive personal information.

2. Minnowing

In this sort of attack, cybercriminals target middle-level employees, but again with very specific targeting tactics. HR people will be targeted with corrupt CVs and the finance department will be sent fake invoices. While it might be their job to always open and action documents, it's important that they watch out for anything that isn't immediately recognizable.

3. Spear Phishing

This is a phishing attack that targets a specific individual within a company, often using information about that individual, garnered from social media or company websites, in order to gain trust. Cybercriminals can target an entire workforce in this way, because personal information is now so readily available, in order to obtain highly sensitive information.

A holistic approach to securing your business against this threat

People

All employees within an organization need to be educated on what a phishing email looks like and the common differentiators to look out for. Some organizations are even working with third party companies to craft fake phishing emails to educate their staff. In this scenario, when an employee does click the 'malicious' link, they are then taken to an informative site to show them what could have happened if it had been a real hacker. While this may be a costly method, it has proven to be very successful as itA both educates staff and provides a platform to monitor your company for weaknesses.

Process

There must be processes in place for employees to follow so phishing attacks cause minimum damage. These processes do not have to be extensive, just something easy to follow and efficient to execute. For example, employees need to notify the IT department of the issue who will then inform the whole company to ensure no further employees fall for the scam. IT can then report it back to the vendor of the spoofed email so they can investigate.

Technology

Next generation email security solutions include **Dual Anti-Virus**, advanced **anti-malware** and **active-code detection** that ensure that no malware comes in, or goes out, via email. Deploying special features such as **Message Sanitization** and **Structural Sanitization** (active code removal) will disable active content from email and attachments to ensure phishing attacks are thwarted at your organization's doorstep. As an extra step, set a policy within your email security solution whereby all external emails are augmented with a message as a reminder for your employees. For example: **'This is an external email. Do you recognize the sender and email address? Think twice before clicking on links or opening attachments'.**

Cyber Etiquette Guide

- Check and double check the email address. Hold your mouse over the sender's name if you can't see the email address outright.
- Always double check any links within the email before clicking on them. Do they look legitimate?
- Check for grammar, spelling and tone of voice within the body of the email. Does the sender always say 'Hi There' like that or sign off with a 'Peace Out'?
- Don't open attachments until you are sure they are legitimate. You can quickly check the title and properties of the document by hovering over it with your mouse.
- Make sure you follow all agreed – and GDPR compliant – processes before transferring any funds or giving any sensitive information. Get in touch with your Data Protection Officer if you're not sure what these involve.
- If you're really not sure, make a call to the genuine sender to see if they did send you the email. If they have been compromised, they will thank you later for bringing it to their attention immediately.
- Notify your organization as soon as possible. The chances are that if one person has been attacked, multiple people in the company will have been too.

#3 SPOOFING: Don't be fooled

What is it?

Spoofing is the act of 'tricking' someone using a false identity. Spoofing as a cyber threat is when a cybercriminal pretends to be someone they are not in order to obtain money, or valuable information, from someone. In the corporate world, this typically manifests itself as a cybercriminal spoofing a CEO, or a CFO's, email address in order to steal funds from a company.

For example, an employee may receive an email in the CEO's name that requests urgent payment to a supplier. The email may include a link to a webpage to enter payment, or asks for credit card details. The employee responds to the spoof request and the cybercriminal will then access the funds, which may never be recovered.

Why is it a threat?

There have been many incidents reported in the media where spoofing has resulted in the unauthorized transfer of significant funds. For example, employees from Medidata Solutions Inc were conned into transferring $5 million to a cybercriminal. The company's insurers initially contested coverage and the matter had to be settled in court. Whilst the final decision found in favour of Medidata, this was some four years after the breach.

An organization's accounts department needs to be particularly vigilant when it comes to spoofed emails, because it's not unusual for this division to receive payment requests. The cybercriminal may even invest time looking online to garner information about an individual's name and role within a company, so the spoofed email is all the more convincing. The criminal may even drop in some other publicly available information, such as customer names.

3 things for businesses to watch out for

1. Tone of voice

While it is relatively easy to set up an email in a CEO's name, it is much harder to imitate their tone of voice. Check for spelling and grammar, in addition to tone of voice. Be wary of any emails that seem out of character or unprofessional.

2. Request

Be suspicious of any email that is requesting something unusual. For example, requesting urgent payment for an invoice, or transfer of funds. Be particularly distrustful if the requested payment method is via a link, or the sender asks for credit card details.

3. Origin of email

A name is not a unique identifier. Anyone can set up an email in the same name as someone else. Therefore, it is important to look at the origin of the email. Check if the email is from a workplace domain, or a personal account. Also check if the email was received at an unusual time, such as very late at night or in the early hours of the morning.

A holistic approach to securing your business against this threat

People

It can be very easy to fool people with a spoofed email, especially if it contains a plausible request. Educate employees about what to look out for and encourage them to report suspicious emails to their IT department. They should also be made aware of who is authorized to process payments and never to send credit card details via email.

Process

Leading high street banks often tell their customers that they will never ask them for sensitive information, such as account details, via email. Adopt a similar approach and educate staff on what they can and can't expect to see in terms of payment requests, and who will send them.

Technology

Next generation spoofing, Business Email Compromise (BEC), requires a **next generation email security** solution to help protect your organization from this threat. Make sure your email security solution has **SPF, DKIM and DMARC functionality** and **allows for custom rules** to be applied to protect employees from BEC. Set a policy within your email security solution whereby all external emails are tagged with a message, for example **'This is an external email. Do you recognize the sender and email address? Think twice before responding, clicking on links or opening attachments.'** Have additional policy checks around emails appearing to come from people with the same names as the executive staff. This will make any spoofed email purporting to be from a staff member look far more suspicious. As an extra precaution, set up the email security solution so that emails that violate compliance policies are quarantined for manual inspection.

Cyber Etiquette Guide

- Check the email address. Does an unusual email that appears to be from your CEO originate from an external, or internal, address? If it appears to be from the company's email domain, are there any subtle differences such as a .co.uk ending, rather than a .com?
- Check the email tone. Be wary of an email that seems out of character in terms of tone, or request.
- Contact the supposed sender, or their team. Ask if they have sent you an email requesting payment.
- Notify your IT department. If you think you've received a spoofed email, ensure you report it straight away.
- Be clear on your company's payment processes. Understand who is authorized to make company payments and who is likely to send requests.
- Never, under any circumstance, send payment details via email.

#4 RANSOMWARE:
The headline-grabbing malware attack

What is it?

Ransomware is a type of malicious software that can be used by cybercriminals to hold an organization's data to ransom. There are two types of ransomware attacks. In the first scenario, through malware, a system becomes locked so no one from within the organization can access it. The second type is where the victim's files are encrypted using a more advanced malware, making them inaccessible while the hacker demands a ransom payment to decrypt them.

Why is it a threat?

A ransomware attack can grind any organization to a halt. For example, the WannaCry incident affected thousands of organizations. In particular, the NHS which had to go back to pen and paper just to keep its services up and running. Once one computer within the network has been infected by the malware, the entire network is soon compromised and the cybercriminal has the ability to encrypt all data and deny access to any information.

3 things for businesses to watch out for

1. Innocuous documents
Constantly looking out for an innocuous document might sound tedious and too open-ended to actually action but 97% of ransomware is delivered to organizations in this way. Watch out for signs such as tone of voice, sender email address and suspicious "click here" actions.

2. Personal emails
Employees opening innocuous documents from a personal account while linked to their corporate network is the main way companies are caught out by ransomware. For example, an employee might receive a recruitment email with a "too good to be true" job specification, that they open out of curiosity and find it contains ransomware too late.

3. Getting stung twice
There is a new generation of ransomware being deployed that hits a company twice as hard as regular ransomware. It has the ability to both steal data as well as encrypt it. This means that an organization must have the data decrypted but once this has happened, there's a strong possibility that the information will still be released to the public as the hacker creates a copy of the data.

A holistic approach to securing your business against this threat

People

When an employee has a ransomware notice pop up on their screen, they can feel very alienated and as if it was all their fault – they often feel as though they will be held responsible for the entire attack. The key here is to make sure employees don't feel too scared to report an attack. The sooner it is reported, the easier it will be to address and manage.

Process

Having policies for all employees to follow around opening documents and personal emails is a must. But whatever you do, never pay the ransom. The likelihood is if you do pay, you still won't get your data back. And if you do get it back, the hackers usually don't remove the malware so the organization will still have to deal with this – including the costs and resources it takes to remove the malware – as well as having paid the hefty price-tag.

Technology

Embedding malicious content within emails and innocuous looking documents is the most common way of being hit by ransomware. Weaponized documents can be made safe with **Adaptive Redaction** technology found in the latest **email and web security solutions**. The **Message Sanitization** and **Structural Sanitization** features enable the automated detection and removal of hidden active code within emails, documents and files, so any malware embedded by hackers is eliminated before it has the chance to infect a network. These features also reduce the human error factor of clicking on malicious links which activates the malware, but it is still important to **train employees** to look for the signs of malicious content.

Cyber Etiquette Guide

- Add technology as a safety net. Install a company-approved ad-blocker to protect your computer from pop-ups that include ransomware, which, like spam emails, can appear to be very authentic in appearance.
- Keep personal affairs off your work device. Never open personal emails on your work computer, there's always a chance it's hiding malicious content.
- Check the sender. Double-check the email address of the sender as this will be the main indicator that the contents of an email is malicious.
- Back-up critical data and files. Where possible, ensure that any critical data you handle is backed-up on a company-approved separate system. This will ensure that if an attack does happen, you won't lose any information.
- Keep your software up-to-date. Ensure you update your computer with the latest software to fix any vulnerabilities that could be exploited. Ask the IT department to set up notifications or auto-updates for this.
- Notify your IT department as soon as possible. If you receive a ransomware notification, don't panic but immediately notify your IT department so they can begin the process of managing the attack.

#5 REMOTE ACCESS TROJANS:
Beware the RATs

What is it?

Remote Access Trojans, or 'RATs', create a backdoor into a computer that allows a cybercriminal remote access to an entire network. Much like the rather unpopular rodent, RATs can cause a lot of damage before detection.

Unlike ransomware, where an employee will instantly know that they have compromised the corporate network, RATs infiltrate the network silently. They gain access to the network through a piece of malware, such as a phishing email.

Why is it a threat?

Once RATs have gained access to a network, they can gain access to any file. They can also use the company network to set up a botnet that sends out spam, or denial-of-service attacks. The cybercriminal can also steel data, and then publish that data, or sell it on.

Sometimes, cybercriminals use RATs in order to target the weakest link in a supply chain. For example, a criminal may want to extract data from a large corporation but can't penetrate the company's security, so instead they target one of the company's suppliers that is easier to hack.

3 things for businesses to watch out for

1. Link clicking
RATs can lurk in links in emails, on webpages, or other documents. Once the link is clicked, malware is activated and the RATs gain entry to the network.

2. Installing apps
Employees can be tempted to download applications that they think will help them during their working day. However, if an app is infected with malware this could compromise the entire corporate network.

3. Bandwidth
Once RATs are in the system they may start sending out large volumes of data, such as spam or company files. Check for any unusual spikes in data usage, or a slowing of the network.

A holistic approach to securing your business against this threat

People

With RATs, an employee is very unlikely to know that they've accidently compromised the company network. Typically, they would have clicked an infected link, or an attachment, and carried on their working day unaware of the consequences of that simple action.

Therefore, it is important that employees know how to avoid compromising a network in the first place. They should be given advice on how to spot a suspicious looking email or document, and the potential consequences of downloading an unauthorized app.

Process

Aside from having security policies in place that help minimize the chances of a breach, a company should also have prepared a cyber breach plan. This should outline the process once an incident has occurred. This may include the need to contact a cyber response team, or even a forensics team, to understand how, and potentially why, the incident occurred. This is especially important if the case needs to go to court and the data needs to be used in evidence.

Technology

It is extremely hard to remove RATs from a network, as they can lie dormant for months and then reactivate. Much like the rodent, they can also find clever places to hide. Therefore, focus should be paid to preventing their entry. **Message Sanitization** and **Structural Sanitization** features built into the latest email security solutions remove hidden active content from email, documents and files, thereby minimizing the chances of an employee clicking on an infected link or attachment. Monitoring of outgoing content can also be used to detect a possible RAT infection.

Cyber Etiquette Guide

- Have a cyber-breach plan in place to deal with incidents swiftly. Ensure people are clear on their roles and responsibilities should a breach occur.
- Check with the IT department before downloading any third party applications.
- Follow basic cyber security best practice. Double check a sender's email address before opening an attachment in an email, or clicking on a link
- Ensure technology is in place that prevents hidden content in emails from being received, and blocks website pop-ups.

#6 DISTRIBUTED DENIAL OF SERVICE (DDoS): The Complex and the Devastating

What is it?

A distributed denial of service (DDoS) attack occurs when a cybercriminal seeks to render a network or an application inaccessible to its intended users by disrupting the services of a host connected to the Internet. DDoS attacks are typically accomplished using botnets that flood the targeted network with surplus requests in an attempt to overload systems and prevent legitimate requests being fulfilled.

In addition to a DDoS attack, an organization can also be attacked via a single source denial of service (DoS) attack, where the incoming traffic flooding the victim originates from a single sources. This is relatively simple to stop as you block traffic from a single source, whereas a DDoS can originate from thousands or tens of thousands of sources.

Why is it a threat?

A DDoS attack can occur on a business's website, email network or any other systems used to communicate with the outside world. When a botnet is attacking the network, it makes it virtually impossible for those outside (consumers, stakeholders) to access it and ultimately will grind businesses to a halt. It is also very cheap to rent a botnet, costing just $100-200 a day, while DIY bot-kits can be purchased for around $20. Therefore, individuals with little skill, time or money but major motives have the ability to cripple any organization.

3 things for businesses to watch out for

1. Cloud

Just because your business might be in the cloud, doesn't mean it can't fall victim to a DDoS attack. Particularly if the cloud provider is small or local, they can be attacked directly, which impacts your business.

2. Website Responsiveness

DDoS attacks start with a degradation of service so it is important to monitor the website for a drop in visitors. This will give an indication that something is amiss and is the major sign that a DDoS attack is on the way.

3. Queue lengths in emails

Another way to determine whether a DDoS attack is on the way is to keep an eye out on external email communications and especially queue lengths. Internally, everything is likely to run as normal but slow external email communications will be an indicator of a DDoS attack. This is because the botnets will hit the open gateway to the point where it cannot cope and slow down processes to deal with so many requests at one time.

A holistic approach to securing your business against this threat

People

It is relatively difficult to educate employees on spotting DDoS attacks as not every employee will be monitoring website traffic, etc. However, it is still important to make them aware of the signs they can look out for – such as slowed email communications – and the effects of an attack. In addition to this, having at least one employee as a member of Cyber Security Information Sharing Partnership (CiSP) will be extremely valuable. The initiative allows for cyber threat information to be shared in real time, ensuring the organization is notified of any DDoS attacks and ultimately allowing them to be prepared.

Process

While most of the processes involved with DDoS attacks happens on the technology side, it's still important to have a human process in place when an attack alert happens. With monitoring systems in place, this will send an automatic notification to the IT department but they often don't do anything with it as they are unsure of who to tell and where to go from there. Implementing a strategy around how to respond to an alert will ensure that the right technologies are implemented and the correct people are notified.

Technology

There are a number of ways a cybercriminal can deliver a denial of service, so there are a number of different ways to defend against an attack. The first technology to implement is a **monitoring service**, which gives you complete visibility of all networks that could be attacked. In addition, **Web Application Firewall (WAF)** is another line of defense as it acts like an antivirus that blocks all malicious attacks on your website. It sits above your application at the network level to provide protection before the attack reaches the organization's server.

Cyber Etiquette Guide

- Be vigilant with checking your email. Keep an eye out for things like emails coming in and leaving the network slowly as this is an indicator that an attack could already be underway.
- Education is key. Stay aware of known and new cyber threats and work with new employees to ensure the whole team is aligned with DDoS.
- Marketing insights. If you work in the marketing department, you will have an overview of website traffic. Ensure you are notifying the appropriate individuals should you see a sudden drop in website traffic.
- Protect your network from BYOD devices. Ensure that users own devices, including IoT and other employee owned devices are on a dedicated network segment, behind a firewall so they cannot infect the corporate network or launch an 'internal' denial of service attack.

#7 SOCIAL MEDIA: Sharing the threat

What is it?

It's hard not to know what social media is – it's absolutely everywhere and part of day-to-day life whether that's for personal or corporate use. Social media has become the go-to platform for businesses to connect with likeminded individuals or groups and promote products and services to a wide audience.

Why is it a threat?

While it is a great source for marketing, recruitment and connecting, social media is a threat to businesses because of this, because everyone uses it. With everyone in a company using social media, especially from a corporate perspective, it is impossible for it to be blocked from day-to-day operations or being used on the network. Therefore, the threat of both individual and company accounts causing a data breach or leakage.

3 things for businesses to watch out for

1. Company spokespeople

Influential individuals within a company – including CEOs and the executives – most likely have their own personal social media accounts. However, if they use this account to promote the organization, it is vital that they extend their professionalism to here. If they are connected to the business and are known to be a key spokesperson, their personal account becomes a reflection on the company. Therefore, sharing drunken pictures of themselves or personal views that do not reflect the company values will be damaging to the company's reputation.

2. Corporate profiles

Ensure that all posts over corporate social media accounts are approved in advance of posting. This will reduce the risk of errors that could seriously damage the company's reputation. In addition to this, it is also important to ensure that any scheduled posts are reviewed in relation to the news agenda as this is another way companies are caught in a reputational issue.

3. Phishing attacks

When employees visit their social media accounts on work devices, they increase the risk of a cyberattack. A post may seem to be legitimate – from a news site or even an individual – to an employee but it could be hiding malware that is activated once it's too late and they have clicked on a link. When the malware is activated, the cybercriminal then has access to the network and ultimately, sensitive data the company holds.

A holistic approach to securing your business against this threat

People

Businesses can't stop employees from using social media at work but can ensure they are well-educated on the threat it poses to a company. Having training sessions on social media best practices can reduce the threat significantly. In addition, influential individuals within the company should be given thorough training on the do's and don'ts of social media as a spokesperson so they know how best to represent themselves and the business online.

Process

There should be policies in place across an organization that ensure social media best practices are being carried out. If there is a designated social media person at a company, they should have the responsibility of maintaining processes such as approvals and messaging that can be used to promote the business to ensure blunders are kept to an absolute minimum.

Technology

Technologies can be put in place to prevent anything damaging being posted on social media. The **latest web security solutions** have the ability to **'monitor' content** as it is being shared on social inside the organization and then accept or change anything that is not appropriate. If it's outside the network then 'external monitoring services' can monitor spokespeople's accounts externally and take down inappropriate content immediately, reducing the chances of policy violating content being seen.

Cyber Etiquette Guide

- Know the limits. Do not log into corporate social media accounts on personal devices and keep personal account off work laptops.
- Be professional. If your personal account is linked to a corporate channel, ensure only appropriate content is being shared as you are an extension of the company and its reputation.
- Password protection. Limit the amount of people who have access to corporate social channels and make sure more than one person has access to the account details.
- Double check content. Ensure if you are posting on the corporate account that you have had the content approved by an authoritative figure. Where possible, stick to pre-determined content to reduce the risk of errors.
- Be GDPR compliant, even on social. Don't take audience data from a channel and store it on your device, this will result in GDPR non-compliance and will cause the entire company to be fined up to €20 million.

#8 PATCHING: First aid for your network

What is it?

Patches are software updates designed to update a system in order to improve it or to fix an issue. All software has vulnerabilities, some of which are obvious and fixed promptly while others have not yet been discovered by companies so are found and exploited by cybercriminals. The main objective of patching is to fix a vulnerability before it is exploited, fix a specific bug, or improve software.

Why is it a threat?

As software and infrastructure becomes increasingly sophisticated and complex, more vulnerabilities will emerge opening up the possibility of an attack from cybercriminals. Many vulnerabilities can lay dormant for years before they're found but as soon as one is discovered, vendors will aim to issue a patch to fix it and protect end-users from potential viruses or malware. However, hackers will also monitor news about patches to determine where vulnerabilities currently lie, aiming to capitalise before users have had a chance to patch their software and protect themselves.

This is also compounded by trends like the emergence of Bring Your Own Device, the Internet of Things and the sheer number of devices that come into the equation as a result. As we operate in an increasingly connected corporate environment, employees work with a range of personal and company devices and applications. This means more things that need to be monitored, patched and repaired regularly, consequently expanding your organization's network attack surface.

3 things for businesses to watch out for

1. Patching news from vendors

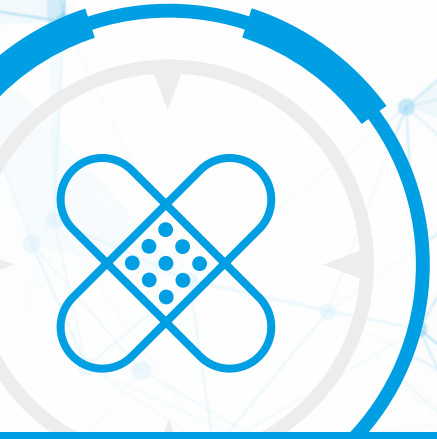
Businesses should keep sight of any patches being released in real-time to be aware of any potential vulnerabilities or updates that would impact business performance. As well as vendors issuing their own updates, there are websites such as the US-CERT current activity web page that can be used to keep abreast of news about patches.

2. Employee personal devices

Every employee device that is connected to the corporate network automatically brings with it another potential avenue for exploitation. With that in mind, organizations have a wider scope of devices and applications to patch to ensure all potential vulnerabilities are addressed.

3. Software update notifications

Employees will often get notifications prompting them to update software, for example with antivirus software. Businesses should ensure that people within the organization are looking out for these and always updating when asked to.



A holistic approach to securing your business against this threat

People

One of the most effective ways to stay protected is to understand the detail within your systems, as this makes finding vulnerabilities and exploits easier. For example, understanding the metadata within documents will tell you which version of software was used.

Organizations should also encourage employees to be a part of this process by communicating and implementing best practice. As well as encouraging employees to make software updates as soon as possible, you may decide to limit the organization's attack surface by asking employees to not use removable media that hasn't been authorised. For example, IBM recently banned employees from using USB sticks because they saw it as a GDPR threat.

Process

The IT team needs to be constantly checking for vendor news and announcements about patches to keep software and systems up to date and avoid vulnerabilities becoming easier to exploit. Rather than simply acting as and when a patch is released, or when a notification about a patch is spotted, a process should be defined and put in place so that patches can be applied in a timely manner. Acting as quickly as possible is key to limiting any possibility of hackers targeting vulnerabilities.

Technology

Having technology in place that helps an organization monitor its environment to keep track of where patches have and haven't been applied to corporate devices is a useful way to assess the company's attack surface at any given time. Companies can also make changes to devices to limit potential threats, for example, changing settings so that USB ports on company devices only enable charging rather than the exchange of data, or changing them so they only enable authorized company devices to connect and transfer information.

Cyber Etiquette Guide

- Keep your software up to date. As soon as a vendor releases a software update or patch, install it straight away.
- Follow protocol. Ensure you follow the clearly defined processes and apply patches quickly and securely.
- Ensure you have stringent control an visibility of all devices and applications - authorized and not authorized - being used in the organization.
- Best patching practice. Ensure you are monitoring for when computers/laptops need updating. This will ensure all devices have the latest security measures in place.

#9 IOT: The Internet of Threats

What is it?

While the Internet of Things (IoT), in a broad sense, encompasses everything connected to the internet, from an iPhone to a smart energy reader. It is increasingly being used to describe task specific machines or objects that communicate with each other without human intervention. The are equipped with real-time data-collecting technologies and analysis. By combining these connected devices with automated systems, it is possible to gather information, analyze it and create an action which can help someone complete a particular task, create business advantage, or unfortunately lend itself to malicious activity.

Why is it a threat?

There is more scope now for devices to be connected to the corporate network, with employees using personal IoT devices such as fitness trackers, all day, every day. Furthermore, when in the home, additional devices can also potentially end up with access to corporate assets. Think of the user querying their Internet connected fridge from the laptop or reading corporate email from a games console. Connecting both personal and corporate IoT devices means there's another set of objects the company now needs to keep up to date with, most of which will go under the radar of the IT department. For example, the organization might patch the corporate iPhones and have a policy that automatically downloads the updates from the app store, but it doesn't have the same process for people's personal android devices – both of which are used as control over IoT devices. IoT is creating an environment where more devices need to be monitored and patched, while also increasing the potential for vulnerability and therefore exploitation. It's not necessarily just the device that's a threat however, but the apps that people use and the back-end systems they feed. Take Strava for example, which leaked information about the location and layout of military bases, all because a number of people linked to the app to track their running routes and times.

3 things for businesses to watch out for

1. Personal connections

Employees bringing their personal devices to work is never a problem. It is when they connect these devices to corporate networks that the security risks start to prevail. Unsecure objects can be hacked 'at home' using freely available tools and then create an issue when they are connected to the corporate network.

2. Kinks in the supply chain

While one organization may have impeccable protocols in place to protect against IoT-based attacks, another company within the supply chain may have weak protective measures which allows an exploit to invade the network. This opens up the entire eco-system to a potential attack and customer data or intellectual property to be stolen.

3. GDPR

Organizations need to recognise the fact that critical data could end up on any personal IoT device if it is connected to a corporate network or allowed access to corporate information. Think about a web browser on a smart TV to read email. With the new GDPR regulations, this could create a data breach so it's important that companies look at the bigger picture to see where its data could end up. For example, if a customer requests to have their data removed (Right To Be Forgotten), and an employee's IoT device is subsequently found to have the data stored on it, the company will be in breach of the regulation. Failing to comply with GDPR can result in significant fines of up to €20M (or 4% annual turnover.)

Securing your devices in the IoT space

People

Education of employees a vital step for any organization to put in place to reduce the threat IoT poses to the business. Many employees do not think about the impact that their personal device(s) can have on the entire corporate network.

Process

Processes that are put in place should be about increasing awareness, with policies around reducing the risk of IoT. This could be as simple as; not connecting your IoT device while on the corporate network, to not using IoT devices at home to access corporate data.

Technology

When it comes to smart phones and laptops, "lock and kill" technologies work well to instantly "kill" or erase the device if it is lost. However, it is only on a small subset of devices compared to the universe of IoT. Within the corporate network, introduce **monitoring solutions** to see what devices are communicating across the boundary, and with what types of information. Also look at **endpoint device management** solutions to ensure all devices within the network follow a definite level of compliance or can only join 'public' networks rather than the corporate one – protecting critical information.

Cyber Etiquette Guide

- Connecting devices. Steer clear of connecting your personal devices to the corporate network.
- Don't get cyber lazy. Ensure all your IoT devices are up to date with security patching and ask your IT department if you're unsure about how to check this.
- Follow protocol. If it's vital that you connect a personal IoT device to the corporate network, ensure you have followed any necessary processes and policies before completing the action. Ask your IT department if you're not sure.
- Don't let the threat fester. If you think you may have compromised the network, notify your IT department as soon as possible. The longer you leave it, the worse the threat becomes.

#10 THE INSIDER THREAT: The Enemy Within

What is it?

Simply put, the insider threat refers to any threat to an organization's security or data that comes from inside the business. This can include direct threats from employees or former employees, but could also include threats from third parties, including contracted suppliers, temporary workers or customers.

There are numerous examples of what could be considered as an insider threat but generally, each threat will fall into two categories, malicious or accidental.

Accidental threats refer to situations where a data breach occurs as a result of the actions of an insider who has no malicious intent. For example, an employee might unintentionally delete an important document, forward an email containing sensitive information to the wrong person, pick up a USB containing malware at an event, share classified information on social media, or even fall victim to a phishing attempt by clicking on a dangerous link within an email.

Malicious threats refer to deliberate attempts by an insider to leak an organization's data or sensitive information. These can be attributed to a rogue employee or ex-employee who believes that they have been wrongfully treated by the organization and are hoping to exact revenge or benefit financially from selling company data.

Why is it a threat?

The insider is a threat to businesses because it can be the cause of a wide variety of threats – such as a breach from a phishing attack or on social media – and is the most common source of a data breach. In 2018, Clearswift's own Insider Threat Index showed that insiders account for 63% of threats, far more than any other threat.

Given human nature, it is very easy for employees to become the unwitting tools of attackers. When met with a protocol that slows down day-to-day tasks, or a process that seems arbitrary and inconvenient, employees can often look for a workaround, ignoring established policies, sharing protocols and data protection procedures.

Employees often jot down passwords on a post-it note, leave computers signed in unattended, and share information without thinking of the wider repercussions from a data security perspective. They may also pick up a USB drive at a show or event that has malware on it, something that can also carry a major security threat. Of course if this is a malicious attack by a rogue employee, the threat can become even more damaging.

3 things for businesses to watch out for

1. Rogue emails to unintended recipients
Clearswift research shows that 45% of employees have mistakenly shared emails containing key data with unintended recipients, including personal information (15%), bank details (9%), attachments (13%) and other confidential text (8%).

2. Security procedures of third parties
Nearly a quarter (24%) of security incidents occur as a result of the actions of those within the extended enterprise, including customers, suppliers and partners.

3. Ex-employee access
More than 13% (one in eight) of all data breaches occur as a result of the actions of employees who no longer work in the business, whether deliberate or unintentional.

3 ways of protecting your business against the insider threat

People

Any good strategy must begin with educating employees about the cyber risks we face today. As 62% of all insider breaches are inadvertent, education is clearly an important part of mitigating this risk. Of course, employees have the potential to make mistakes but highlighting their own ability to cause a data breach and how they can minimize this risk can foster a culture of good data hygiene.

Process

Organizations should take stock of the various policies, procedures and processes that are currently in place and look to plug any gaps. This includes giving training and guidance on what to do when something goes wrong such as "Who do I talk to if I think I've clicked on a malicious link or opened a suspicious attachment that I shouldn't have?"

Technology

Technology should then act as a last line of defense to limit the potential effects of any mistakes that slip through the net or highlight where any malicious activity is taking place. Technology should ensure an organization can enforce the policies and procedures that have been put in place, to protect the people both within the organization as well as customers and any third parties a company works with. **Adaptive Data Loss Prevention technology** and its associated functionality offers the greatest chance to **mitigate data leaks and emails sent in error**. However, no matter what solution is right for your company, a chief consideration must be that any security solutions that IT deploy, must be focused on **protecting individuals** to make sure that, if they do make a mistake, the impact of that mistake is minimized.

Cyber Etiquette Guide

- Follow the guidelines. A clear and concise handbook of policies and controls should be created and given to each employee.
- Training is key. Arrange educational sessions and ensure employees are receiving training that reflects their day-to-day role.
- Know your data. Where possible, co, collect a clear picture of where the critical data you handle sits and map out its journey so if a breach happens you can notify the right people promptly.
- Technology isn't the silver bullet. Adopting an appropriate Data Loss Prevention (DLP) solution that monitors employee actions can stop any mistakes but following good data practice will ensure the insider threat is reduced further.

clearswift
by HelpSystems

Clearswift is trusted by organizations globally to protect critical information, giving teams the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to gain visibility and control of their critical information 100% of the time.

Adaptive Data Loss Prevention

Unparalleled Inspection and Redaction. No False Positives. No Disruptions.

Email Security

Unevasive Detection and Sanitization. Adaptive Security & Data Loss Prevention for email.

Web Security

Beyond Filtering. Adaptive Security & Data Loss Prevention for the web and cloud applications.

Endpoint Protection

Data secured. Devices secured. Risk mitigated.

Information Governance and Compliance

Track,Trace and Secure. Real-Time Policy Enforcement.

For more information, please visit **www.clearswift.com**