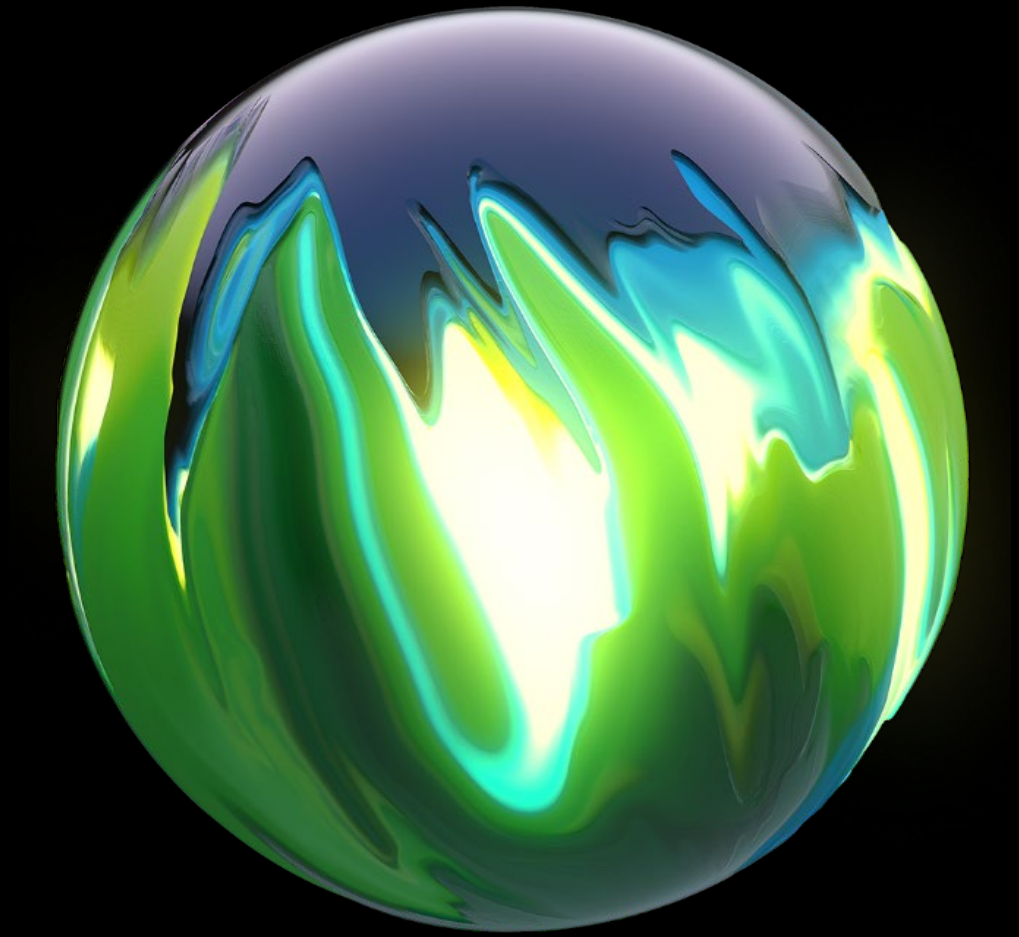
Deloitte.



Cybersecurity trends

A discussion with Cayman Compass
November 3rd , 2021

MAKING AN IMPACT THAT MATTERS since 1845

Our Speakers

Dr. Alexandra Forssell
CISSP, CIPM, PMP, ISO 27001 Lead Auditor,
Ph.D. in Information Assurance and Security

Risk Advisory Director
asimonova@deloitte.com
(345) 743-6333

Wayne Green
CISSP, CEH, ISO 27001 Auditor, GIAC
GCIH, GIAC GSEC

Risk Advisory Director
wagreen@deloitte.com
(345) 743-6256

October was Cybersecurity Awareness Month

Do Your Part. #BeCyberSmart

Introduction

Cyber Threats, Ransomware, Cost of Cybercrime

Cyber Threats

If we start with a global baseline from data collected by the Identity Theft Resource Center (ITRC):

- The healthcare sector has suffered the most breaches the past three (3) years including the first quarter of 2021
- Non-Profit, Professional Services and Retail are some of the “sectors” with the largest growth in individuals affected by breaches while hospitality and transportation showed declines
- The data also shows the most successful attacks start with credentials obtained via email phishing attacks

Top Spoofed Brands

Microsoft
Amazon
Apple
Zoom

Targeted Industries for Phishing Attacks

Healthcare
Real Estate
Chemicals
High Tech
Education
Outsourced Service Providers

Mitigation: Phishing attacks can be mitigated by continued awareness training and by being vigilant

Source: “Notified,” Identity Theft Resource Center

Ransomware

For the last couple of years ransomware attacks have included data exfiltration:

- It is no longer an availability issue
- Backup and restore capabilities are required but are not a complete solution
- It is crucial not to panic and have a plan

A typical ransomware attack chain

Mitigation: Continued education and awareness about phishing, detecting common tools and renamed executables

Source: SANS 2021 Top New Attacks and Threat Report, Deloitte: Taking data hostage - The rise of ransomware

Cost of cybercrime

FBI's IC3 Internet Crime Report (2020) showed that losses from internet crimes increased from $1.5B (2016) to $4.2B (2020), with phishing seeing the highest growth

Verizon's Data Breach Investigations Report (2021) showed that business email compromise breaches cost on average between $250 to $984,855

Source: 2021 Data Breach Investigations Report | Verizon, IC3 2020 Internet Crime Report

How to be Cyber Safe

A New Paradigm, Collaboration Security, Mobile Device Security, Online Security Basics, Social Media Security

The evolution Cyber Resilience | A new paradigm

The function of managing and regulating cyber risk has evolved into a new paradigm that includes four central and strategic components.

Governance

Establish a vision and strategy, roles and responsibilities, as part of the management function of cyber risk and information security. Including considerations for the particular business, laws and regulations, human resources, and technology.

Secure

Focus on the protection of information and the technology that supports key business processes, implementing adequate controls for the risks and threats to the organisation.

Vigilant

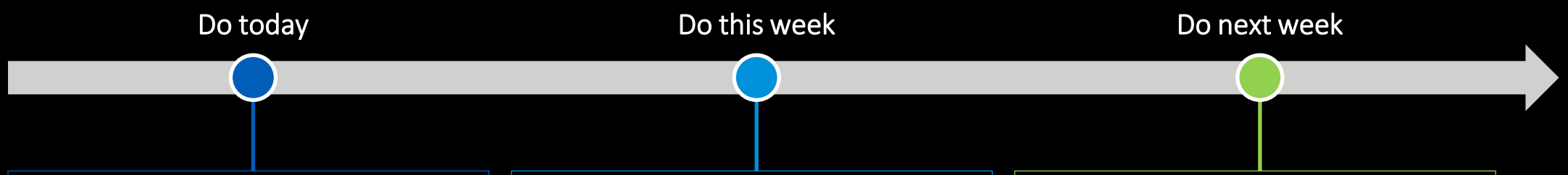
Look to establish a culture across the organisation that calls attention to the threats and develop the capabilities to detect patterns of behaviour that could indicate, detect, or predict an attack.

Resilient

Build the capability to rapidly control the damage and mobilise necessary resources to minimise the impact to include direct costs, business disruption, and reputational brand damage.

Source: *Cyber Risk services | Boost your cyber strategy, security, vigilance, and resilience*.
Retrieved from https://www2.deloitte.com/ky/en/pages/risk/articles/cyber-risk-in-cayman.html

Collaboration security activities to consider



Do today

- Enforce auto generated password use for meeting access
- Enable meeting waiting rooms and lock meetings once they have begun
- Disable custom meeting IDs and passwords
- Disable the ability to integrate with third-parties and social networks
- Request (from platform provider) that meeting codes be expanded to at least nine digits.

Do this week

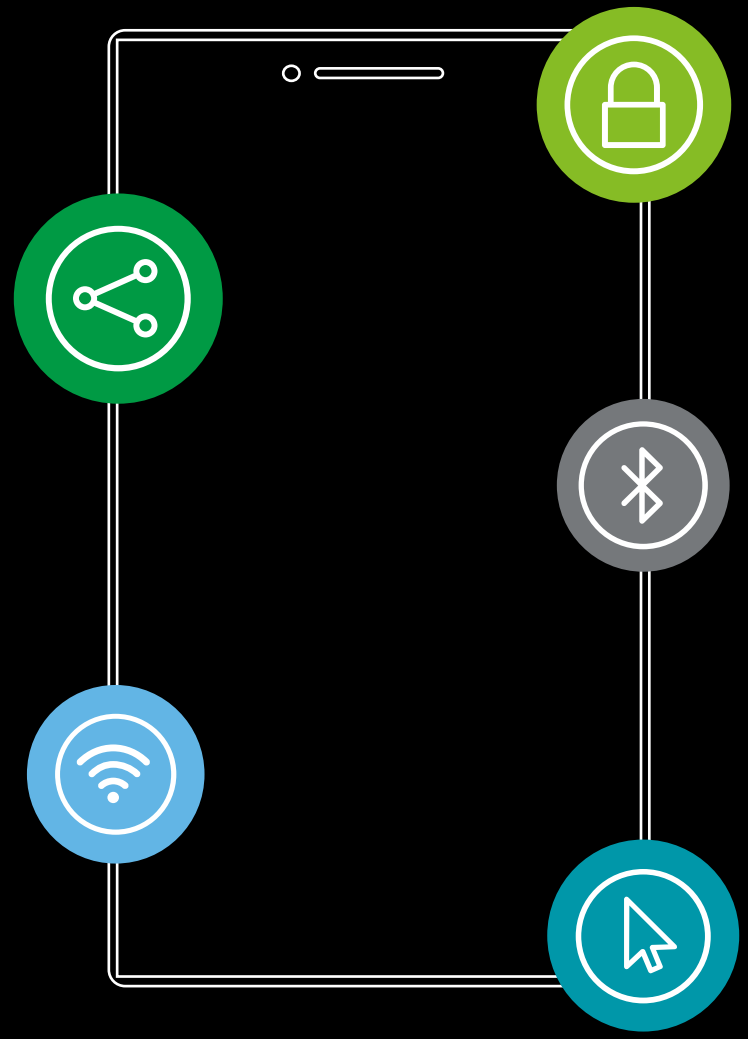
- Maintain and enforce organization's guidelines on platforms regarding meeting password access, meeting recording policies, and content transmission on the platform
- Push security awareness training for organization meeting hosts to reinforce secure collaboration practices, such as setting expiration dates for recorded meetings.

Do next week

- Reissue meeting invitations as needed to include additional security layers
- Enable Single-Sign-On to consistently enforce authentication rulesets
- Contact platform provider for additional information on specific organisational security requests and controls.

Mobile device security

Here are some simple tips to protect your mobile device:



Passcode-protect your device

Enable strong passcode protection on your device and include a timeout requiring authentication after a period of inactivity. Secure your smartphone with a unique passcode.

Update the operating system

Smartphones are computing devices that need to be updated. Updates often provide you with enhanced functionality and enriched features, as well as fixes to critical security vulnerabilities.

Disable Bluetooth devices when not in use

Bluetooth capability can provide ease and convenience in using your smartphone, but it can also provide an easy way for a nearby, unauthorized user to gain access to your data.

Be cautious with public Wi-Fi

Many smartphone users use free Wi-Fi hotspots to access data. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.

Think before you click

Before responding, registering, downloading or providing information, get the facts. If the download is not from a legitimate app store or the site of a trusted company, do not engage with the message.

Top security mistakes people make with their mobile device

Mobile devices have advanced us into a new era of productivity and working on-the-go. But with those advances and added convenience comes many security blunders just waiting to happen. Here are some of the worst security mistakes you can make with your mobile device and how to avoid them.

1

Failing to lock down your device

- The first line of defense is locking your device. This can be the differentiating factor that keeps your lost or stolen phone protected long enough to track it down or wipe it remotely.

2

Not having the most up to date versions of your apps

- Apps are often released with vulnerabilities, and sometimes those security flaws even manage to persist throughout multiple updates of the software. Keeping your software up to date by downloading updates as soon as possible after they are released can prevent potential security risks caused by using outdated apps.

3

Opening questionable content

- There are a number of ways you can access questionable content via your mobile device. Messaging poses a particular threat in the form of spam texts containing malicious links to sites. Equally risky is downloading apps from third-party app stores. When you download software from untrusted sources that are not, for example, Google or Apple approved, there's no telling what kind of malicious software you may end up with.

4

Using public or unsecure Wi-Fi

- When it comes to using Wi-Fi instead of your phone's data connection, stick to what you know is secure, like networks with WPA2 encryption. Open, unprotected networks are entirely too risky, especially for users that are carrying sensitive company data on their devices. Aside from making it all too easy for others to access your mobile device's information by sharing the same network, public Wi-Fi can even allow attackers to hijack your device through your apps.

Bluetooth security

Many electronic devices are now using Bluetooth technology to allow wireless communication with other Bluetooth devices. Before using Bluetooth, it is important to understand what security risks it presents and how to protect yourself.

Depending on how it is configured, Bluetooth technology can be fairly secure, but if someone can "discover" your device, they may be able to send you unsolicited messages or find a way to access or corrupt your data. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

1

Disable Bluetooth when you are not using it

- Unless you are actively transferring information from one device to another, disable the technology to prevent unauthorized people from accessing it.

2

Use Bluetooth in "hidden" mode

- When you have Bluetooth enabled, make sure it is "hidden," not "discoverable." The hidden mode prevents other Bluetooth devices from recognizing your device.

3

Be careful where you use Bluetooth

- Be aware of your environment when pairing devices or operating in discoverable mode. For example, if you are in a public wireless "hotspot," there is a risk that someone else may be able to intercept the connection.

4

Take advantage of security settings

- Examine your security settings and select options that meet your needs without putting you at increased risk. Make sure that all of your Bluetooth connections are configured to require a secure connection.

Good home wireless network security

Practicing good wireless network security can help reduce the risk of your home network being compromised. Here are some tips you can follow to secure your home network:

1

Change your wireless network name

- While not a security issue by itself, revealing your wireless network name will facilitate nefarious actors identifying the make and model of your home router and thereby allowing them to potentially determine if the device is vulnerable.

2

Disable WPS (Wifi Protected Setup)

- This feature was found to have a vulnerability a number of years ago but remains enabled by default on many routers.

3

Turn off guest networking

- In certain circumstances home routers have a Guest access feature enabled by default. This negates the need for a security key when accessing a wireless network.

4

Choose a strong security protocol

- Ensure you select “WPA2” or the newer “WPA3” for your router’s wireless network security protocol, and make sure your password is hard to guess.

Good online security practices

Practicing good online security habits can help reduce the risk of your computer being compromised. Here are some tips you can follow to stay safe online:

1. **Use and maintain anti-virus software**
   - Anti-virus software recognizes and protects your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage.
2. **Use a firewall**
   - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer and limiting the traffic you send.
3. **Use strong passwords**
   - Select passwords that will be difficult for attackers to guess. Use different passwords for different programs and devices. Do not choose options that allow your computer to remember your passwords.
4. **Keep software up to date**
   - Install software patches so that attackers cannot take advantage of known problems or vulnerabilities.
5. **Use caution when online**
   - Take appropriate precautions when using email and web browsers to reduce the risk that your actions will trigger an infection. Think before you click.

Tips for staying safer online

Practicing good online security habits can help reduce the risk of your computer being compromised and increase the protection of your data. Here are three tips to help you stay safer online:

Make sure that the URL of the website begins with https (not http). Https helps to ensure that your username, password, credit card number, expiration date and other information are sent from your computer to the site in encrypted form. Encryption helps to make your connection secure and reduces the risk that malicious people may intercept the information you enter and make illegal use of it.

A yellow icon that looks like a padlock at the lower right corner of your browser window confirms that you have a secure connection.

Some websites present a certificate of authenticity when you browse to them as a way to assure you that the site is legitimate. Check to make sure the certificate is valid and has not expired. If you are satisfied with the validity of the certificate, click on the link that takes you to the site itself. An invalid or expired certificate may indicate that the site neither authentic nor secure.

Understanding website certificates

By making sure a web site encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to gather your information. If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure web site, your browser will check the certificate to ensure that the web site address matches the address on the certificate and the certificate is recognized by the browser as being signed by a "trusted" authority.

If the browser senses a problem, it may present a dialog box that claims there is an error with the site certificate. If you are unsure whether the certificate is valid or question the security of the site, do not submit personal information.

How do you check a certificate?

A secure way to verify the information about the certificate is to look for the certificate feature in the menu options. This information may be under the file properties or the security option within the page information. You will get a dialog box with information about the certificate, including the following:

- Who issued the certificate - The issuer should be a legitimate, trusted certificate authority.
- Who the certificate is issued to - The certificate should be issued to the organization who owns the web site.
- Expiration date - Most certificates are issued for one or two years. Be wary of organizations with certificates that are valid for longer than two years or with certificates that have expired.

Keeping children safe online

When a child is using your computer, normal safeguards and security practices may not be sufficient. You may think that because the child is only playing a game, or researching a term paper, or typing a homework assignment, he or she can't cause any harm. But what if, when saving their paper, the child deletes a necessary program file? Or what if they unintentionally visit a malicious web page that infects your computer with a virus?

What can you do?

Be involved

Consider activities you can work on together. This will allow you to supervise your child's online activities while teaching them good computer habits.

Monitor activity

If your computer is in a high-traffic area, you will be able to easily monitor the computer activity. Be aware of what your child is doing on the computer, including which websites they visit.

Set rules and warn about dangers

Make sure your child knows the boundaries of what they are allowed to do on the computer, including how long they are allowed to be on the computer, which sites they are allowed to visit, what software programs they can use, and what tasks or activities they are allowed to do.

Keep lines of communication open

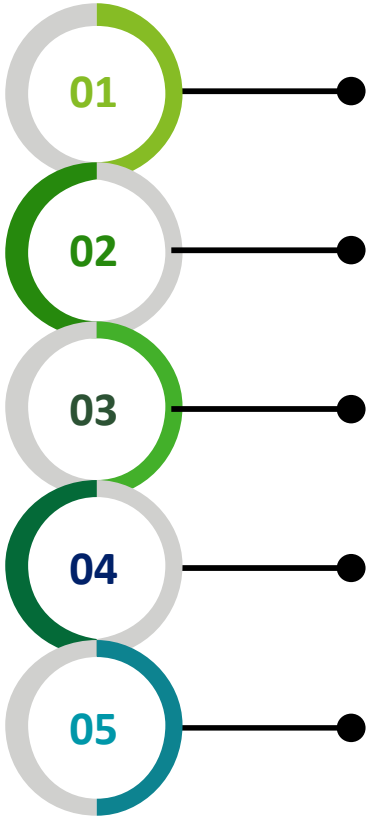
Let your child know that they can approach you with any questions or concerns about behaviors or problems they may have encountered on the computer.

Consider partitioning your computer into separate accounts

Most operating systems give you the option of creating a different user account for each user. If you're worried that your child may accidentally access, modify, and/or delete your files, you can give them a separate account and decrease the amount of access and number of privileges they have. If you don't have separate accounts, you should be especially careful about your security settings. In addition to limiting functionality within your browser, avoid letting your browser remember passwords and other personal information.

Safety when shopping online

The internet offers a convenience that is not available from any other shopping outlet. From the comfort of your home, you can search for items from countless vendors, compare prices with a few simple mouse clicks, and make purchases without waiting in line. However, the internet is also convenient for attackers, giving them multiple ways to access the personal and financial information of unsuspecting shoppers. Attackers who are able to obtain this information may use it for their own financial gain, either by making purchases themselves or by selling the information to someone else. Take precautions with personal information and follow these recommendations to minimize your risk and **do business with reputable vendors!**



Use security settings software
Passwords and other security settings add layers of protection if used properly.

Check privacy policies
Take precautions when giving personal information, and make sure to check published privacy policies to see how a company will use or distribute your information.

Be careful what information you share
Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums.

Use anti-virus software and a firewall
Protect yourself against viruses by using anti-virus software and a firewall. Make sure to keep your virus definitions up to date.

Be aware of your account activity
Check your bank and credit card statements regularly and your credit report at least yearly.

Staying safe on social media sites

Some tips to help protect yourself when using social media sites:

Personal information 01

Limit the amount of personal information you post

Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing.

Posting content 02

Remember that the internet is a public resource

Only post information that you are comfortable with anyone seeing. This includes information and photos in blogs and other forums. Once you post information online, you cannot retract it. Even if you remove the information from a site, saved or cached versions may still exist on other's computers.

Privacy Settings 03

Evaluate your privacy settings

Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so do not post anything you do not want the public to see. Sites may change their privacy options periodically, so review your security and privacy settings regularly.

Privacy Policies 04

Check privacy policies

Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam.

Thank you!

Do Your Part. #BeCyberSmart

Deloitte.