YOUNG INTERNAL AUDITORS SUMMIT

Future Leaders Adapting to New Landscape

The Institute of Internal Auditors Philippines YIAS 2021

Cyber Security and Data Privacy in the Expanded Work Environment

Carmelo R. Alcala, FICD

AGENDA

- Overview
- The Pandemic Came
- Key Issues in the Pandemic
- Threats for Employers and Employees
- The Phishing Landscape
- Scams and Malware
- Staying Safe
- Common Warning Signs of a Cyber Attack
- Protecting the Company
- The New Normal
- Key Takeaways
- The Final Word

Profile - Carmelo Alcala, Senior IT GRC Manager, Connor-Consulting (US)

FICD, CDPSE, CISA, CICA, CrFA, CPISI, Cobit5F, ISO31000RM, ISO27001LA, ISO27032LCM

- 30+ years combined professional experience in Corporate Governance, Internal Audit, Risk Management, IT GRC and Compliance. 10 years in an IA Leadership role.
- Fellow of the Institute of Corporate Directors (ICD)
- Member, Technology Governance Committee of ICD
- Member, Joint Cyber Security Working Group (JSCWG)
- PECB-Accredited lecturer on ISO31000 Risk Management and ISO27001 ISMS (Montreal, Canada)
- SEC-Accredited lecturer on Corporate Governance
- ISACA lecturer on Risk Management, Data Privacy, ISO27001, CISA Reviewer
- ICD Teaching Fellow on Corporate Governance, Audit, Risk Management, IT Strategic Governance and Data Privacy
- GRI- Certified Trainor on Sustainability Development Reporting

Directorships:

- Independent Director and Compliance Consultant, Geniusto Philippines (Fintech)
- Independent Director, Exceture, Inc. (IT Consulting)
- Board of Trustee, ISACA-Manila (2010-2019) (Non-Profit)
- President and Chairman, ISACA-Manila (2013-2014)
- Board of Director, NPC Employees Coop (2003-2012)

Overview

Cybersecurity

- Are measures taken to protect a company's IT ecosystem against unauthorized access from a hacker.
- Focuses on specific technical implementation needed to protect the IT system
- The most common forms of cyber attacks are phishing, spear phishing and injecting malware code into a computer system.

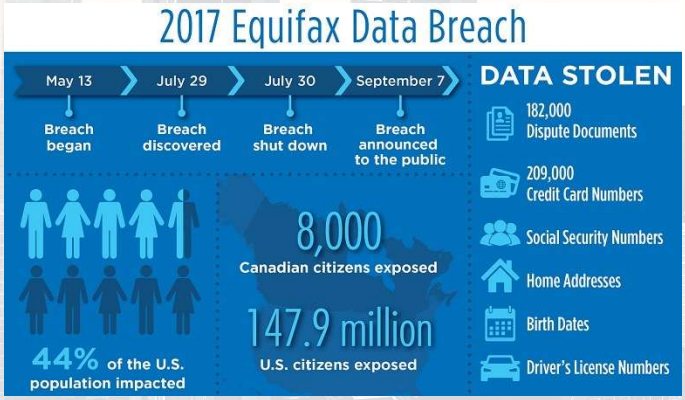
Cybersecurity in the News

Overview

Data Privacy

- Data protection is a set of procedures aimed at safeguarding personal data stored within a system.
- It is a consumer's understanding of their rights as to how their personal information is collected, used, stored and shared.
- Data protection addresses data management, availability, unauthorized access prevention and application regulations like RA10173, HIPAA, CCPA, or GDPR.
- A type of "information security that deals with the proper handling of data concerning consent, notice, sensitivity and regulatory concerns."

Data Privacy in the news



Why Data Protection And Cybersecurity Can't Be Separate Functions

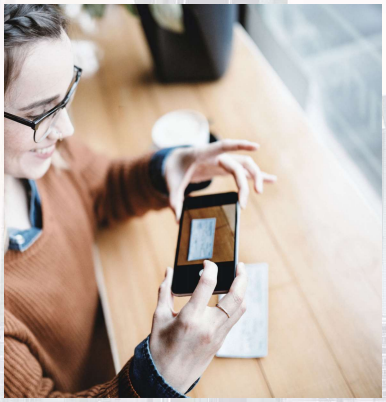
- Data breaches affect various aspects of an organization's data life cycle, including its IT environment and processes.
- There is a need to oversee both data and systems at the same time to ensure coverage of the organization's vulnerabilities and exploits.
- Both data protection and cybersecurity deal with protecting data from various digital and IT threats. That's why they have become interconnected.


AND THEN COVID19 HAPPENED…


Sorry
WE'RE
CLOSED


LOOKING
FOR A
JOB

Key Issues in the Pandemic



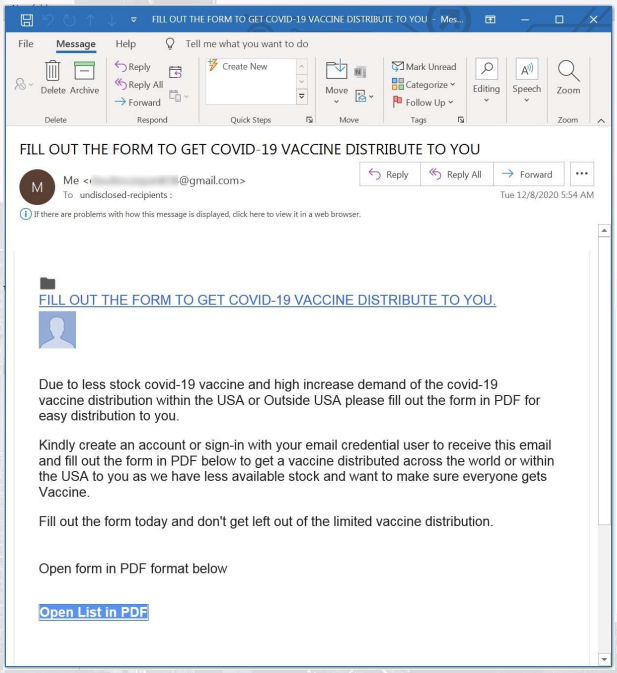
- Operational resilience
- Treating customers fairly
- Employees
- Reputation management
- Regulatory and compliance obligations

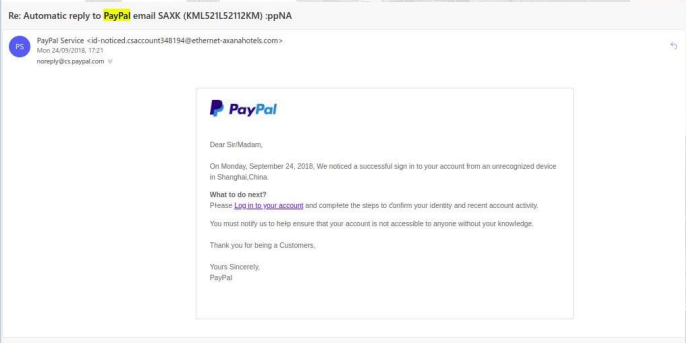
https://www.addleshawgoddard.com/en/insights/insights-briefings/2020/financial-services/the-challenge-for-the-challenger-banks/

Employee Threats during the Pandemic

Social Engineering

- An attack vector that relies on human interaction
- Involves manipulating people into breaking normal security protocols, procedures in order to gain access to computer systems, networks or physical locations for financial or other gain
- Designed to lure unsuspecting users into providing business confidential and personally identifiable information (PII).
- Once the data are obtained, cybercriminals then attempt to infect computer systems and networks with malware by opening links to infected sites, sending e-mail or texting scams and attachments containing computer viruses and network worms, phishing and pharming hooks, and encouraging the overall use of public networks, mobile device apps, and infected external drives.





Employee Threats during the Pandemic

Human error

- The primary threat to companies' data security, increased by the remoteness and lack of adequate cybersecurity planning for teleworkers.
- Careless employees, consultants, vendors, and other stakeholders can also pose danger to cybersecurity
- Employees abandoning routine security practices when working from home

Threats during the Pandemic

Management Failure

- Inability to recognize, plan, and fund adequate teleworker measures,
- Consistently manage backup networks, hardware, software, communication equipment, and storage devices
- Adequately train employees to recognize and report pretexting overtures and cyberattacks
- Development and training of WFH policies and procedures
- Update traditional cybersecurity strategies, lacking the vital technology necessary to detect and stop attackers already within a system or network
- Excessive access to valuable organizational data by employees (more access than needed) just by logging into their work computers.

The Phishing Landscape

“An emotional response justifies many people actions when they are phished and is exactly what hackers are looking for.”

Covid Phishing Threat Landscape (2019-2020)

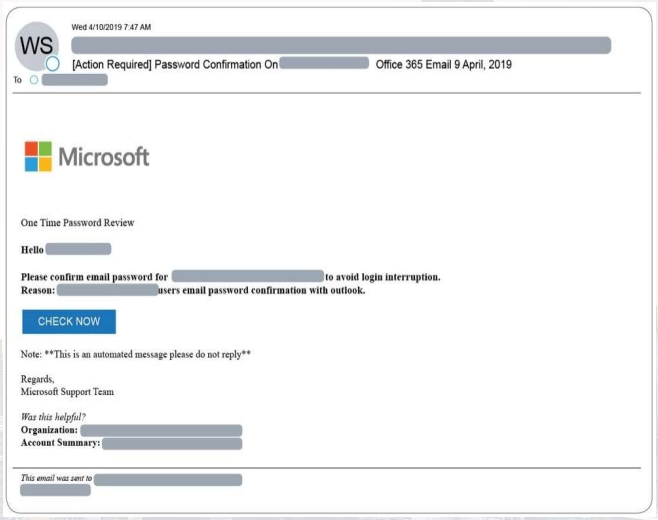
$26.2B	42.8%	667%	30%	32.5%
Losses from business email compromise(BEC) attacks	of malicious attachments were Microsoft Office documents	Increase in phishing scams in only 1 month during the pandemic	Of phishing messages were delivered on mondays	Of all the emails used the keyword 'Payment' in the email subject

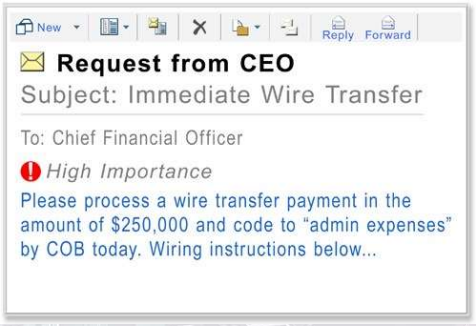
https://www.enisa.europa.eu/publications/phishing

Phishing Kill Chain

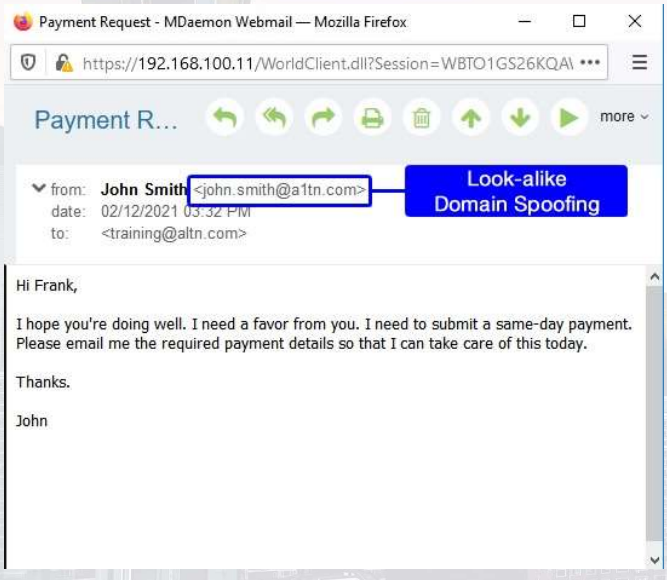
Business Email Compromise

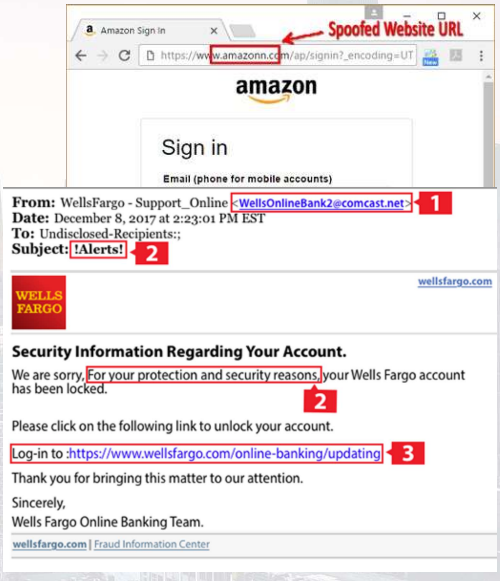
- 86% of worldwide organizations faced BEC attacks
- Most targeted to harvest credentials – Microsoft 365
- Once data have been collected, attacker can impersonate an employee, CEO or trusted supplier to divert funds to third-party accounts



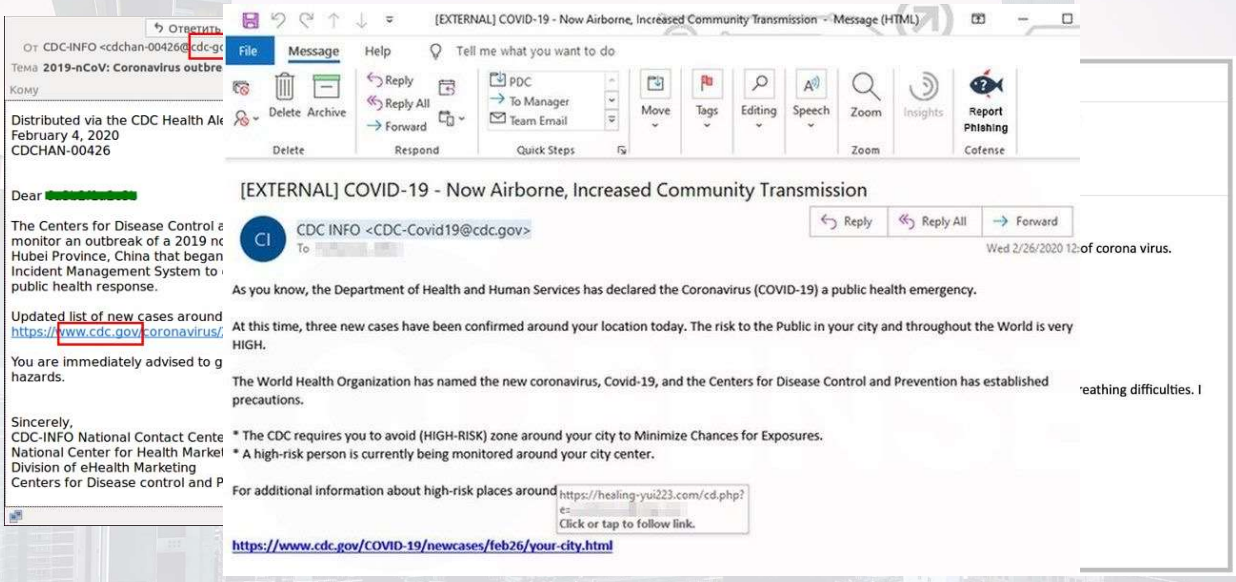


74% of phishing sites also use HTTPS





COVID-19 used as a phishing lure



[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission - Message (HTML)

File Message Help Tell me what you want to do

Reply Reply All Forward Delete Archive PDC To Manager Team Email Move Tags Editing Speech Zoom Insights Report Phishing

[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission

CDC INFO <CDC-Covid19@cdc.gov>

Reply Reply All Forward

As you know, the Department of Health and Human Services has declared the Coronavirus (COVID-19) a public health emergency.

At this time, three new cases have been confirmed around your location today. The risk to the Public in your city and throughout the World is very HIGH.

The World Health Organization has named the new coronavirus, Covid-19, and the Centers for Disease Control and Prevention has established precautions.

* The CDC requires you to avoid (HIGH-RISK) zone around your city to Minimize Chances for Exposures.
* A high-risk person is currently being monitored around your city center.

For additional information about high-risk places around

https://healing-yui223.com/cd.php?

Click or tap to follow link.

https://www.cdc.gov/COVID-19/newcases/feb26/your-city.html

Scams

Subject: YOUR URGENT SUPPORT IS NEEDED

Charset iso-8859-1 *

Hello,

Good Day,

The death toll from the monthlong coronavirus outbreak has continued to climb in 27 Countries rising to 870 Cases.
New cases have surged by double-digit percentages in the past 14 days, with no sign of a slowdown,due to lack of individual consign.
More people have now died in this epidemic than in the SARS outbreak of 2002-3 in mainland China.
Health communities in the world have
Organized a Fund rising program (US$675 million is needed) to support the control of the epidemic in Noneremote areas in the world.
Let's save Humanity: Your support is needed.

WORLD HEALTH COMMUNITY BITCOIN WALLET FOR DONATION IS BELOW,

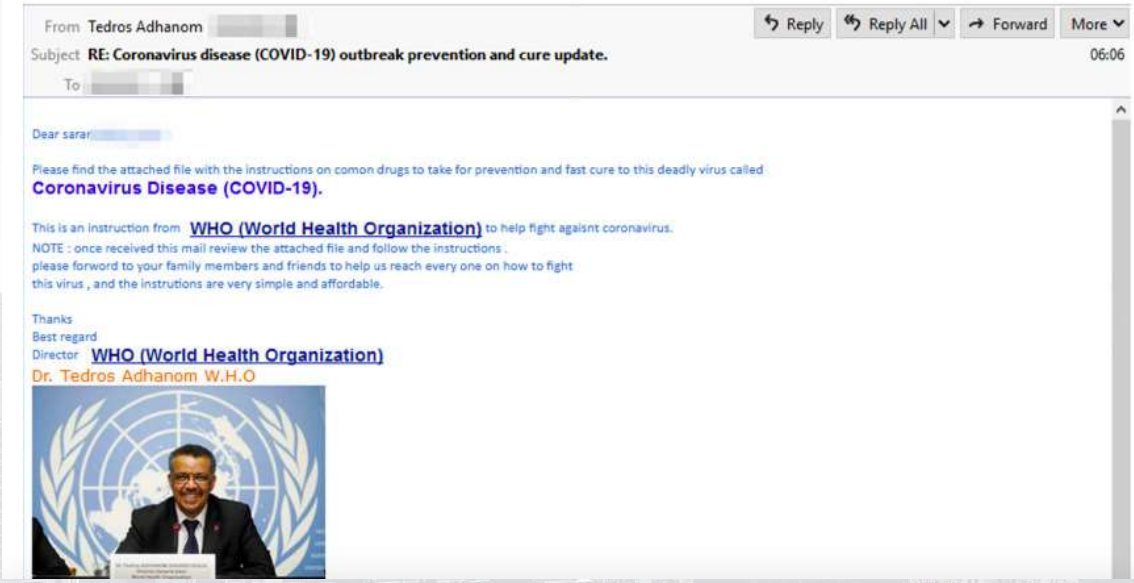
BITCOIN WALLET DETAILS: 1JTpX5T4ks9vfL1yaftL1Z3LisDdatkSQC

No amount is too small.

Thanks and Best Regards
Hugo Yeung
Support Committee Member
World Health community
+8606430910,+8037535467

- Sell coronavirus cures or face masks
- Asking for investments in fake companies that claimed to be developing vaccines

The Info-Stealer Disguised in World Health Organization Theme



https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

Malware

Subject: RE: Corona - Impact of Shipment - Details required -- High Priority -- TOP URGENT REMINDER 1
Charset utf-8 *

Good day,

With the current impact with COVID-19 (Corona Virus Impact), we would like to know the production/delivery status of our orders with you.

Kindly fill the details in attached template for each of the given orders which is pending to ship and send to us by tomorrow – 04 March.

Awaiting your priority cooperation.

Best regards,
Amanda Chen
****

Amanda Chen / 陳宗明 (Ms.)
PTT (Taiwan) Co., Ltd.
台灣進達科貿股份有限公司
12F-1, No.129, Section 2, Zhongshan North Rd.,
Taipei 10448, Taiwan
10448台北市中山北路二段129號12F-1 (吉美大樓)
TEL: 02-8751-5818 Ext.217 FAX: 02-8797-7809
E-mail: amanda.chen@ptttw.com.tw
****

Ransomware

Staying Safe while WFH

Staying safe while WFH

- Use antivirus and internet security software
- Keep away family members from work devices
- Invest in a sliding cam cover
- Use a VPN
- Use a centralized storage solution

Staying safe while WFH

- Secure your home Wi-Fi
- Beware of Zoom and video conferencing
- Make sure your passwords are strong and secure
- Protect your online banking
- Beware of email scams and your email security

Common Warning Signs of a Cybersecurity Attack

Common Warning Signs of a Cybersecurity Attack

- MONITOR UNUSUAL BEHAVIOR
- INVESTIGATE SUSPICIOUS FILES
- REVIEW SYSTEM COMMUNICATIONS
- RUN SCANS
- CHECK YOUR CREDIT

Protecting The Company from a Cybersecurity Attack

Making your company safe from Cyber Attacks

Keep Data safe

staff should only have access to the information vital to their particular role

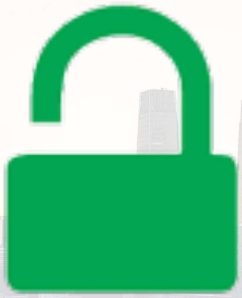
consider records retention programs – require destruction of data in a proper manner by employees from their computers including hard copies

Data should be archived or deleted based on local and international laws

Making your company safe from Cyber Attacks

Password Protection Program

- use strong passwords for every site accessed on a daily basis
- should never be shared between employees or written down where others can see it.



81%

of breaches leveraged **stolen** or **weak** ** passwords **

(Verizon Data Breach Investigations Report 2017)

Making your company safe from Cyber Attacks

Update Security Software

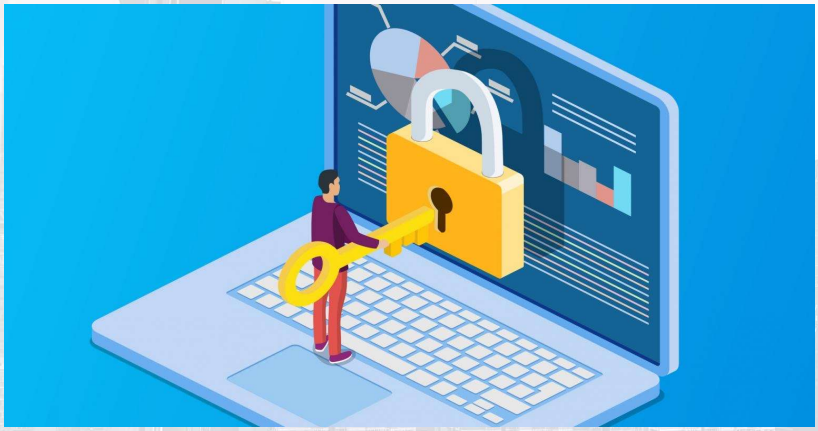
- Utilize firewalls, anti-virus software and anti-spyware programs to help ensure sensitive data cannot be easily accessed by hackers.
- Security programs also require regular updates to keep them free from vulnerabilities, so make sure to check any software vendors' websites to learn about upcoming security patches and other updates.

Making your company safe from Cyber Attacks

Employee Training:

- All employees should be trained on the importance and methods of data security.
- Both physical and digital records should be safeguarded at all times
- Confidential information about clients, employees or corporate affairs should always remain secured.

Making your company safe from Cyber Attacks



Data Encryption:

- All data, whether on a personal device, computer, or server should be protected by proper encryption.
- Companies can benefit from safe harbor exemptions that only apply if the company can prove the data was encrypted before a breach
- Use encryption software to protect company data by barring access to any unauthorized users

Making your company safe from Cyber Attacks

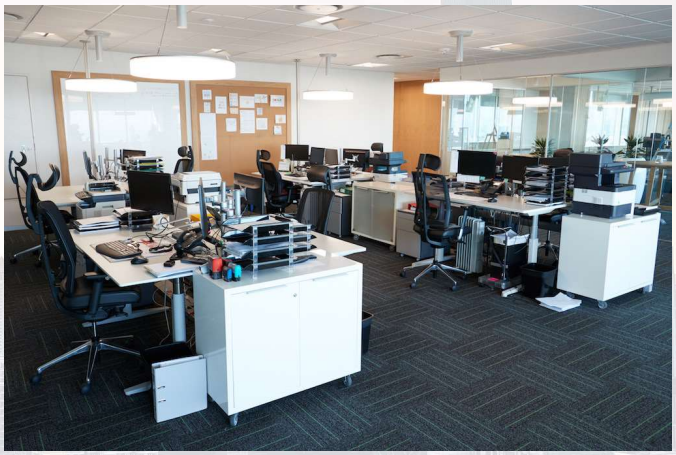
- Have a documented WFH Security Policy
- Have a BYOD (Bring Your Own Device) policy
- Provide cyber security awareness training to employees
- Train staff to be alert to phishing attacks and how to avoid falling victim to them
- Encourage the use of two-factor authentication to validate credentials
- Advise staff to use corporate email solutions and not to rely on their own email or messaging accounts for the storage or transmission of personal data
- Include cyber and data privacy in your risk management and business continuity
- Assess your 3rd party risks and include them in your audit universe

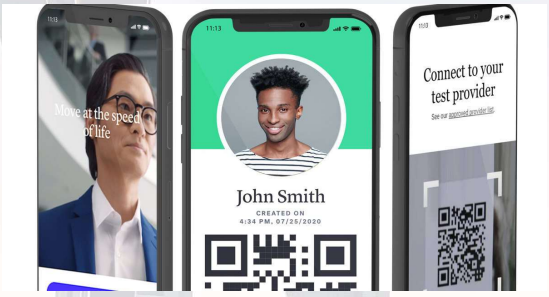
The C Elements to Develop an Inclusive WFH Corporate Culture

- Control
- Collaboration
- Communication
- Cost
- Cloud
- Culture

The New Normal - Are you ready to return to your office?

- Finding an array of tech-infused gadgetry to improve workplace safety
- Temperature checks, distance monitors, digital “passports,” wellness surveys and robotic cleaning and disinfection systems are being deployed in many workplaces seeking to reopen.
- Tech giants and startups are offering solutions that include computer vision detection of vital signs to wearables that can offer early indications of the onset of COVID-19 and apps that keep track of health metrics.





[Health Pass | CLEAR (clearme.com)]

[Digital Health Pass | IBM]

[Fitbit, Inc. - Fitbit Introduces Ready for Work Solution to Help Employers Manage Workplace Health and Safety During the COVID-19 Pandemic]

[ProtectWell Home page - ProtectWell (weprotectwell.com)]

The New Normal

- A delicate balance of ensuring workplace safety without intruding on privacy for employees, visitors, etc.
- Conflicts between requiring proof of vaccination and restricted access to employee's health data
- Increase reliance to third party tech vendors to handle health and safety monitoring and management
- Fingerprint recognition, face recognition, voice recognition and other technologies collect user information to provide users with convenient and efficient services,

Take Aways

- WFH presents a serious vulnerability to cybersecurity and privacy threats.
- WFH initiative demands support, buy-in, and funding from the most senior levels of the organization and must be extended to all stakeholders.
- Cybersecurity protection for teleworkers starts with robust ethics training and security education programs.
- In the event that cyber intrusions are successful, it is critical to employ a process or solution that can both eliminate infections and track their source
- Protecting the organization from being victimized by hackers and social engineers must be the responsibility of each and every employee, regardless of location..
- We must all be vigilant to protect against the scourge of encrypted malicious traffic from hackers and social engineers, *regardless of where we telework*.

The Final Word

- Cybersecurity and privacy training and monitoring has to be a major plank of the WFH platform.
- Organization's leaders must re-assess the business continuity and infrastructure plans to operationalize WFH as a normal (not a-typical) practice.
- Adequate technology must be assessed and acquired, routinely patched
- Employees should be consistently motivated with innovative training programs, communication media, and incentives.
- Organizations may develop and perform a WFH Cybersecurity Knowledge Management Program, starting with an audit to learn both the explicit and tacit information already established for remote employees.
- Imperative to learn what is known and not known, prior to commencing the development of an important new WFH enterprise-wide initiative.

Q & A

Thank You

meloalcala@gmail.com
linkedin@carmelo-alcala

References

- https://amtrustfinancial.com/blog/small-business/cybersecurity-vs-data-privacy
- https://www.securitymagazine.com/blogs/14-security-blog/post/94568-cybersecurity-risk---increased-by-the-pandemic---redefines-the-workplace
- https://www.enisa.europa.eu/publications/phishing
- https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/
- https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html