HERBEIN
CPAS + CONSULTANTS

Information Security Risk - Considerations For A Remote Environment

1.855.HC.Today | www.herbein.com

LEGAL DISCLAIMER

The webinar will remain live for ten additional minutes after the conclusion of the presentation to provide the opportunity to submit follow up questions via the Q&A function. A summary of top questions may be provided to all attendees.

Additionally, all attendees will be emailed a link to a recording of the webinar, a pdf of the presentation, and speaker bios and contact information.

Today's presentation is not:

- Legal advice
- The final word on today's topics – updates will be continuously provided via herbein.com
- Qualified for continuing education credits (i.e. CPE.)

Before taking any action, companies should check with their internal and/or external advisors

Today's Presenters

Jeff Johns
Partner
Financial Outsourcing Solutions
A subsidiary of Herbein + Company, Inc.
jjohns@fosaudit.com

James Michalak
Partner, Chief Information & Digital Officer
Herbein & Company, Inc.
jamichalak@herbein.com

Poll Question #1

Has COVID-19 changed your working environment from a technology perspective?

- ❑ Yes
- ❑ No

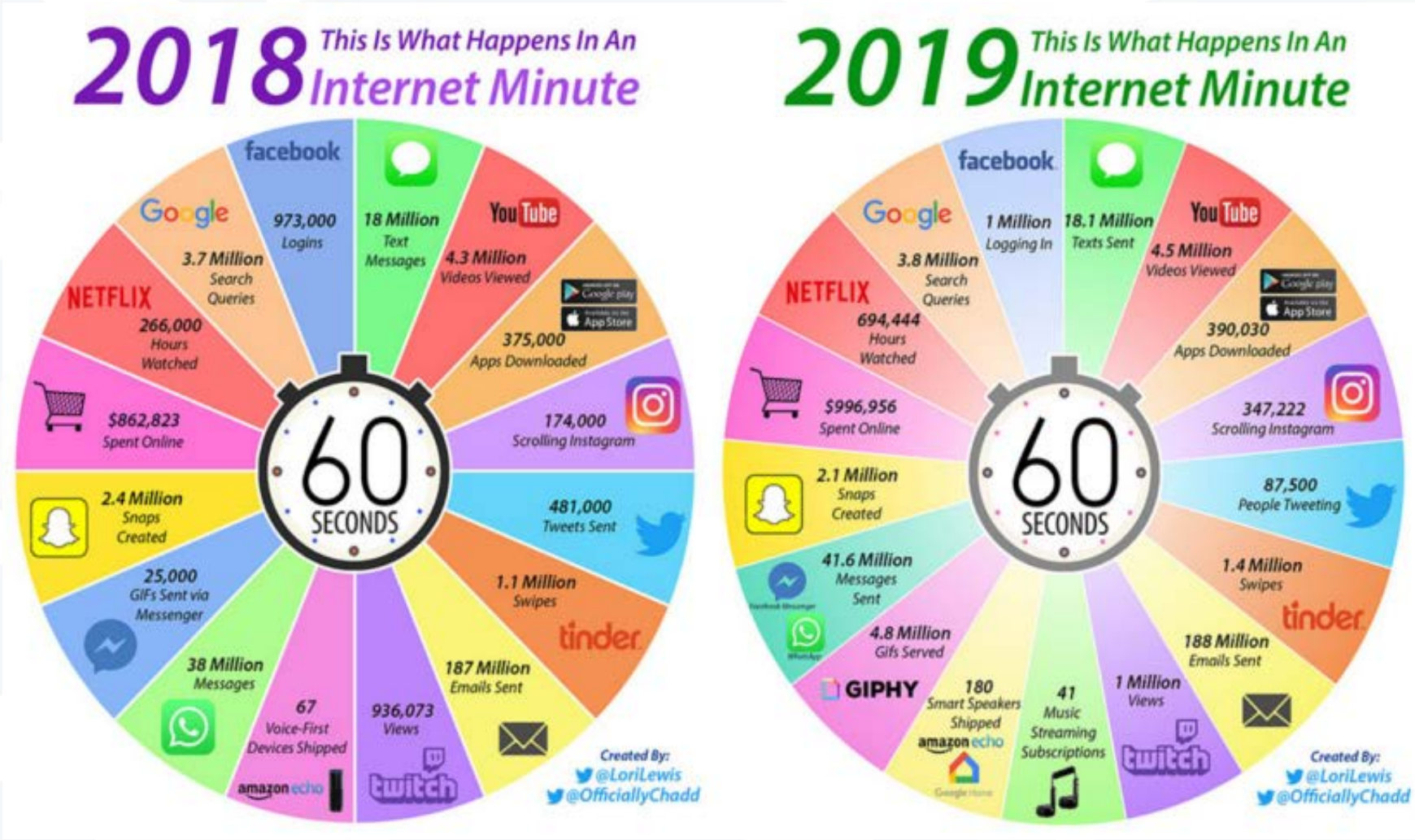
COVID-19 REALITY

ATTACKS ARE INCREASING

- 26% are seeing increased attacks
- 73% believe that the impact of this pandemic will alter the way their business evaluates risk for at least the next five years

WORK FROM HOME IS A NEW CHALLENGE

- 61% were more concerned about security risks targeting WFH employees
- 22% evaluating new security solutions/services to address the new work dynamic


2018 This Is What Happens In An Internet Minute
60 SECONDS
facebook
973,000 Logins
18 Million Text Messages
YouTube
4.3 Million Videos Viewed
375,000 Apps Downloaded
174,000 Scrolling Instagram
481,000 Tweets Sent
1.1 Million Swipes
tinder
187 Million Emails Sent
936,073 Views
twitch
67 Voice-First Devices Shipped
amazon echo
38 Million Messages
25,000 GIFs Sent via Messenger
2.4 Million Snaps Created
$862,823 Spent Online
NETFLIX
266,000 Hours Watched
Google
3.7 Million Search Queries
Created By:
@LoriLewis
@OfficiallyChadd
2019 This Is What Happens In An Internet Minute
60 SECONDS
facebook
1 Million Logging In
18.1 Million Texts Sent
YouTube
4.5 Million Videos Viewed
390,030 Apps Downloaded
347,222 Scrolling Instagram
87,500 People Tweeting
1.4 Million Swipes
tinder
188 Million Emails Sent
1 Million Views
twitch
41 Music Streaming Subscriptions
180 Smart Speakers Shipped
amazon echo
4.8 Million Gifs Served
GIPHY
41.6 Million Messages Sent
2.1 Million Snaps Created
$996,956 Spent Online
NETFLIX
694,444 Hours Watched
Google
3.8 Million Search Queries
Created By:
@LoriLewis
@OfficiallyChadd

COVID-19 Security Events

- A senior US Secret Service official estimates $30 billion in stimulus funds will be stolen through COVID-19 scams.

  Secret Service has taken steps to counter these scams and has prevented around $1 billion from being lost to malicious actors.
- The FBI on 6/10/2020 warned that malicious cyber actors were targeting mobile banking apps in an attempt to steal money as more Americans have moved to online banking during the coronavirus pandemic.
- In a public service announcement, the FBI noted it expects to see hackers “exploit” mobile banking platforms, which have seen a 50 percent surge in use since the beginning of the pandemic.

COVID-19 Security Events

Microsoft is warning of an ongoing COVID-19-themed phishing campaign mirroring the Johns Hopkins Center. The massive campaign is spreading via malicious Excel attachment.

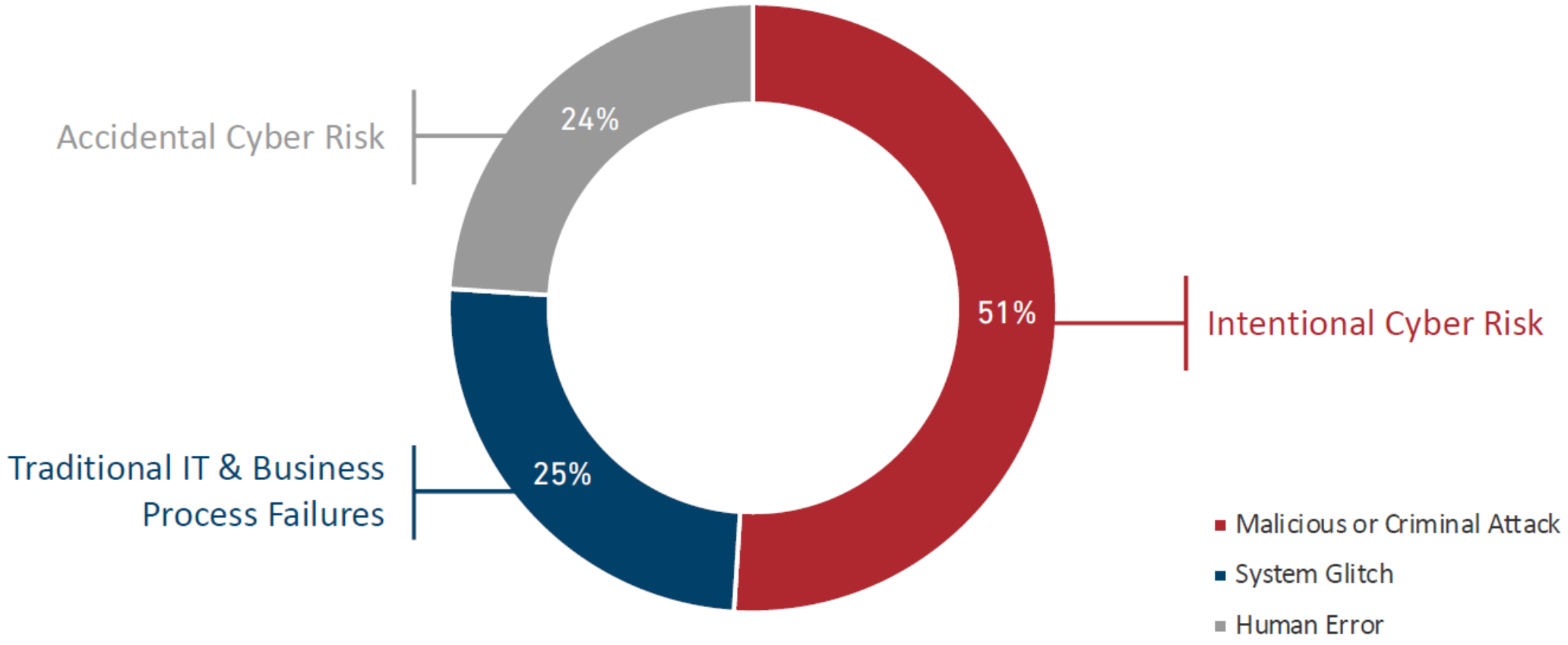
- The attachment contains macros that prompt the user to “Enable Content” and once clicked, will download and install the NetSupport Manager client.
- NetSupport Manager is a legitimate remote administration tool and is commonly distributed among hacker communities to use as a remote access trojan.
- When installed, it allows a threat actor to gain complete control over the infected machine and execute commands on it remotely.

Polling Question #2

How concerned are you that your Company is at risk of a cyber related event (data breach, phishing attack, etc)?

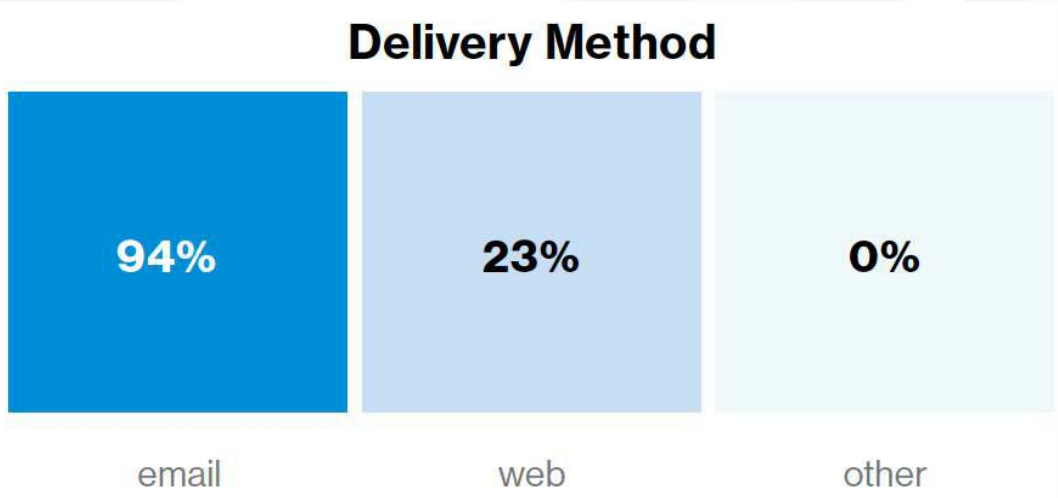
- ❑ Very Concerned
- ❑ Somewhat Concerned
- ❑ Not Concerned At All

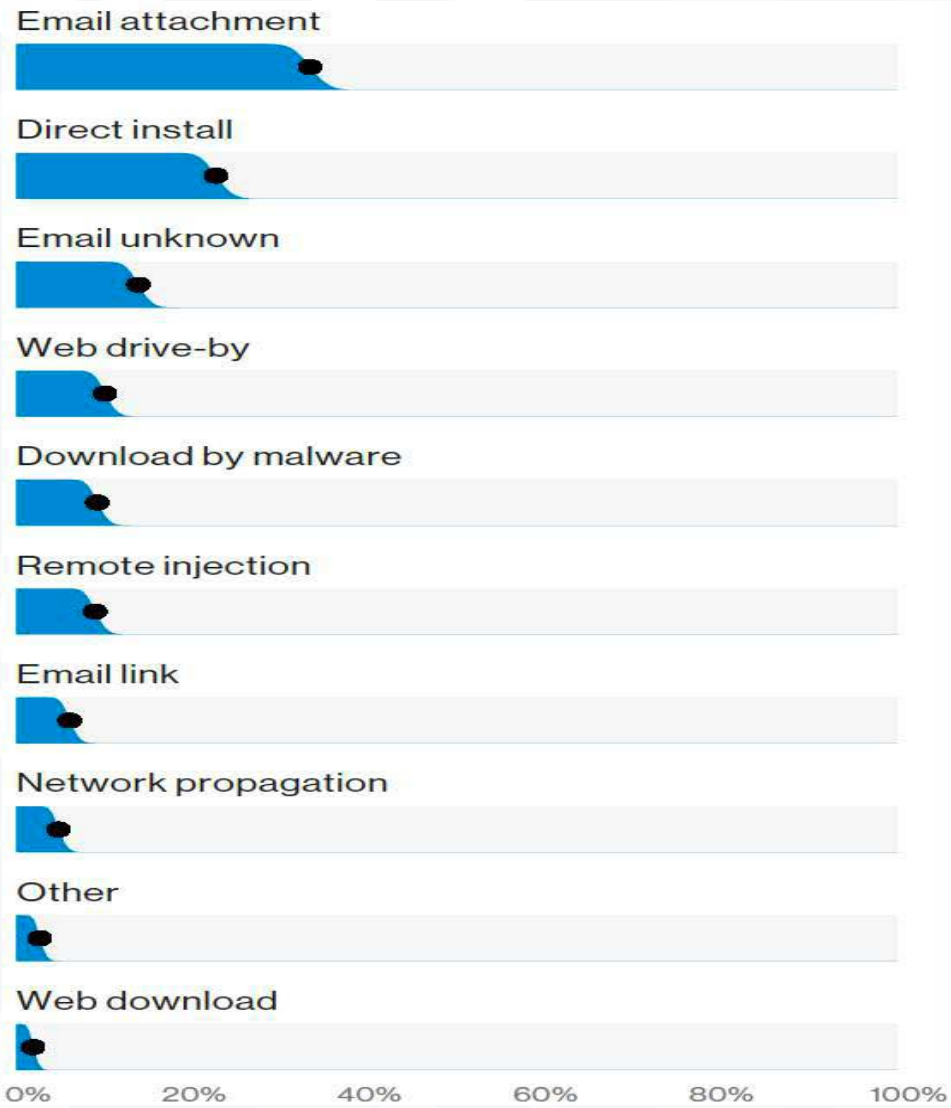
Root Cause of Data Breach



Source: "2019 Cost of a Data Breach Report," Ponemon Institute - 2019

Email & Malware





Today's Reality

3.1 billion + phishing emails were sent every day.

Source: Forbes

Spam messages accounted for 57.26 percent of e-mail traffic in December 2019.

Source: statista.com/

March 2020: Unsafe Clicks From COVID-19-Themed Email Phishing Attacks Nearly Double In Recent Weeks; Mimecast Blocks Up To 5,000 URLs Related To The Coronavirus A Day—37x What We Blocked In January.

Source: Mimecast

More than 136,000 new COVID-19 themed domains were observed between 12/1 and 3/27.

Source: Spycloud

Phishing crackdown sees 2,000 Coronavirus scammers taken offline

by SophieDowdell — April 21, 2020 in Cyber Bites

As the number of cyber criminals targeting remote workers grows, the National Cyber Security Centre has kicked off a new effort to encouraging people to report suspicious emails in an attempt to crack down on fraudsters and phishing scams. The coronavirus pandemic has led to record numbers of organisations requiring people to work from home – and in many cases, those employees haven't had any previous experience of working remotely and could be unaware of some of the potential security risks.

Source: ZD Net

Case Study

Office 365

Work or school account

someone@example.com

Password

Keep me signed in

Sign in

Can't access your account?

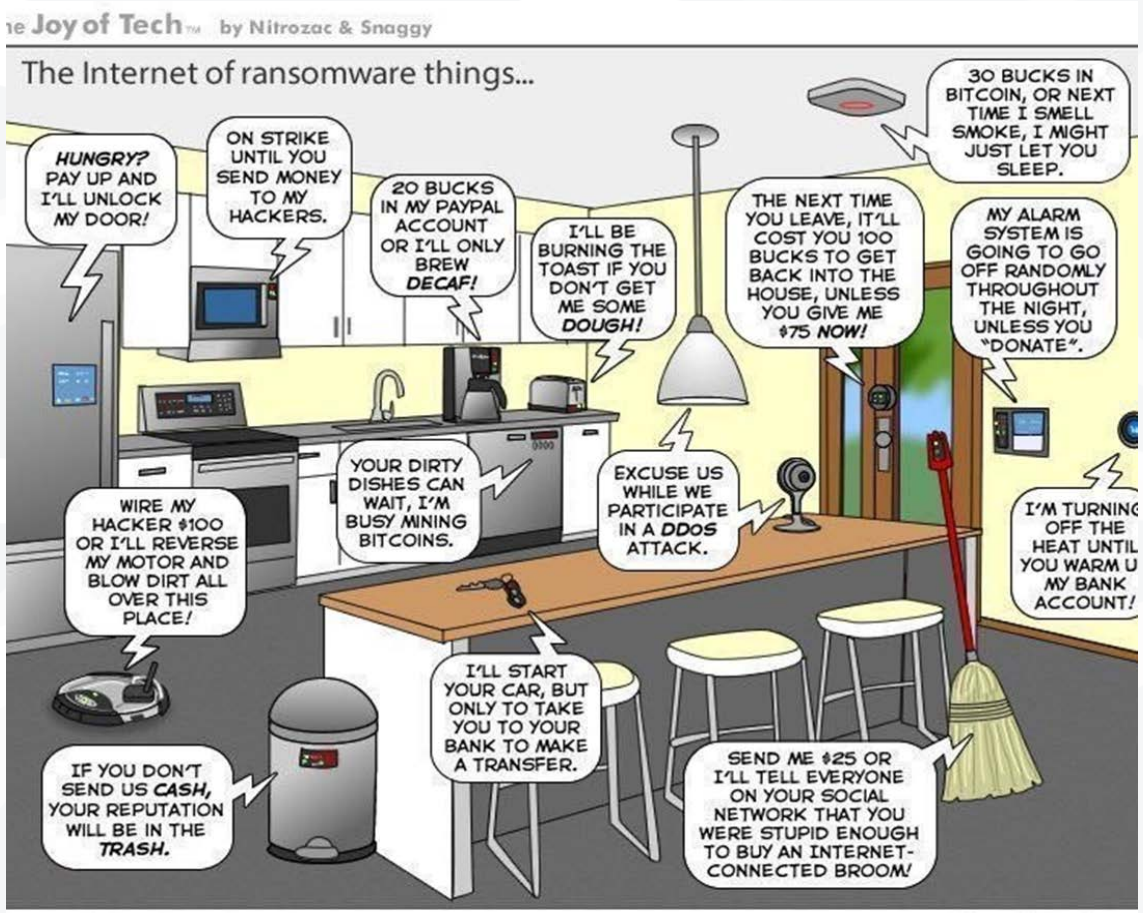
© 2017 Microsoft

Microsoft

IT Challenges in a COVID-19 World

- Decentralized workforce
- Remote workforce readiness (laptops, infrastructure, etc)
- Device management
- Rapid deployment of remote tools
- Complexity causing lack of configuration
- Productivity vs Security
- Staffing shortages

Cyber Risk Exposure Only Continues to Grow



- More devices attaching to networks
- Wider variety of devices
- Much more extensive use of technology
- More sophisticated users
- Rapid adoption of technology
- Skills Gap

Polling Question #3

Has your organization performed a review of IT level controls?

- ❑ Yes, Annually
- ❑ Yes, Several Years Ago
- ❑ No, Considering One
- ❑ No, We feel secure
- ❑ I Do Not Know

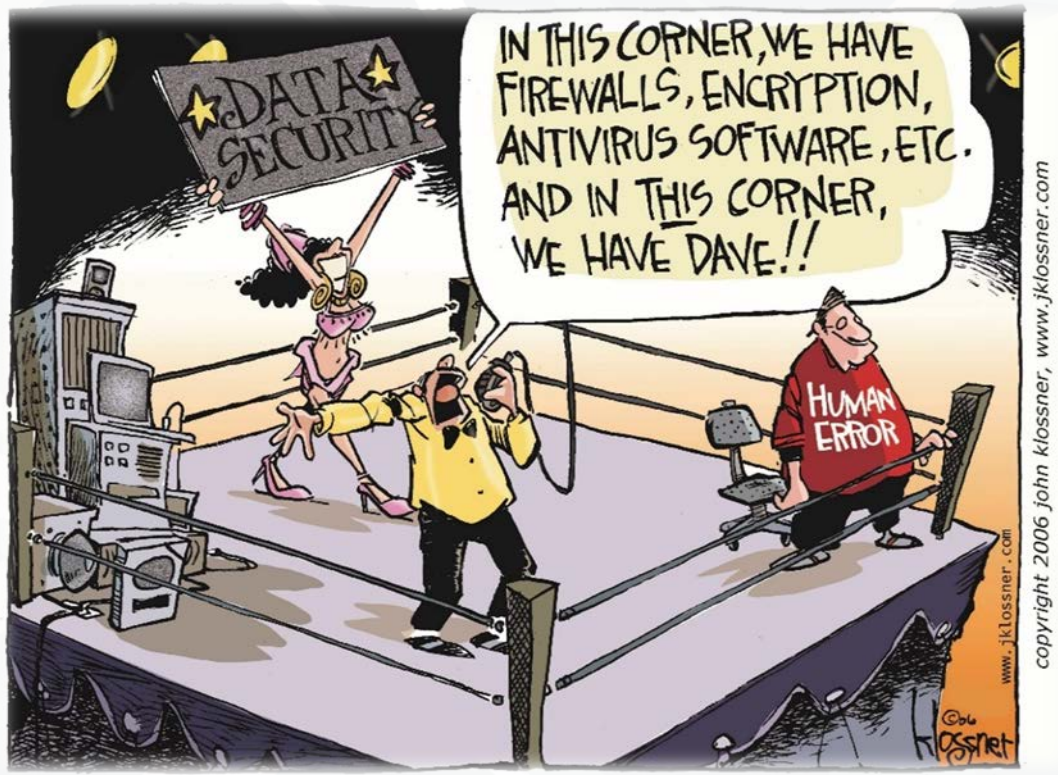
Strengthen Your Cyber Posture

Protection of Key Data

- ✓Know your data
- ✓Information security practices and policies
- ✓Incident response program and training
- ✓Employee training and awareness
- ✓Insurance coverage (i.e. cyber security)
- ✓Vendor management program
  - ✓ Initial and periodic review process
  - ✓ Storage and transmission of sensitive information
  - ✓ Information security practices
  - ✓ Insurance coverage

Recommendations For The Protection Of The Systems

- ✓ Perimeter level security
- ✓ Limit the use of unmanaged or personal devices
- ✓ Stringent administrator level requirements (least privilege)
- ✓ Application level of access restrictions
  - ✓ User rights
  - ✓ Limit accessibility outside of the network
- ✓ End user controls
  - ✓ Strong password requirement with 2 factor authentication
  - ✓ Virus, malware, spam protection
  - ✓ Means for secure communication
  - ✓ Mobile device / remote access restrictions
  - ✓ VPN & multifactor authentication access for remote users
  - ✓ Encryption
- ✓ Network and system monitoring
- ✓ Vulnerability Management
- ✓ Security Awareness Program



No news is often bad news. Oversight and accountability is key. Reports, metrics and data should be regularly reviewed.

Video Conference Recommendations

- Do not make meetings public
- Use meeting passwords and/or use the waiting room feature to control the admittance of guests
- Utilize a meeting lock which stops newcomers from joining once everyone you were expecting has arrived
- Do not share the link to publicly available websites such as social media pages; instead, send the meeting links directly to invited participants
- Always make sure you are using the latest version of the application and install updates to your apps as soon as they are made available
- Be aware of the information being discussed and shared
- Review the recommended security settings for video conference platform and ensure they are enabled

Cyber Security – A Business Perspective

- ✓ It's not a matter of will it happen, but when – are we reasonably prepared?
  - Reasonable information security safeguards and monitoring in place
  - Adequate insurance coverage
  - Adequate education efforts
  - Oversight over the administrators
  - IT Accountability

- ✓ Are my stakeholders aware of the importance and reputational risk – management, board, IT?
- ✓ Fort Knox doesn't exist – what's a good business balance?
- ✓ Responsibility can't be delegated – do I know what my vendors do with my data?
- ✓ Knowledge and education are key!

Key Questions To Ask

- ✓ What are the top risks our organization faces?
- ✓ Do we have an effective security awareness program?
- ✓ In the event of a data breach, what is our response plan?
- ✓ When did we last test our recovery/response procedures?
- ✓ How to stay on top of vulnerabilities?
- ✓ Who is holding IT and/or our MSP accountable?
- ✓ Do we have adequate safeguards?
- ✓ Do we need an independent review of our IT controls environment?

Additional Resources

Herbein IT Risk Management Services

- https://www.herbein.com/services/consulting/it-risk-management

Microsoft Teams

- https://docs.microsoft.com/en-us/microsoftteams/teamssecurity-guide

Zoom

- https://zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf

Office 365

- https://docs.microsoft.com/en-us/microsoft-365/security/top-security-tasks-for-remotework?view=o365-worldwide

Risk Management Framework (RMF) -NIST

- https://csrc.nist.gov/projects/risk-management/riskmanagement-framework-(RMF)-Overview

Microsoft: Data Classification for Cloud Computing

- http://aka.ms/dataclassificationforcloud

Final Thoughts…

HERBEIN
CPAS + CONSULTANTS

The webinar will remain live for ten additional minutes to provide the opportunity to submit follow up questions via the Q&A function. A summary of top questions will be provided to all attendees, if appropriate.

Additionally, all attendees will be emailed a link to a recording of the webinar, a pdf of the presentation, and a listing of speaker biographies and contact information.

Thank you for attending our webinar!