Mid-Atlantic CIO Forum

Shawn King CISSP®
Chief Architect for Cyber, Digital Twin, & Edge Computing
Dell Technologies Public Sector

Email: shawn.k@dell.com
@linkedin 1shawnmking
@twitter   @1shawnmking

DELLTechnologies

Agenda

- Cyber Trends in the midst of a Pandemic

- Increasing Threat Surface

- Compliance and Security Framework Standards

- Mitigating Cyber Events

- Board Room Discussion

https://sli.do
R823 to join the presentation.

DELLTechnologies

Cyber Trends in the midst a Pandemic

- 1 out of every 3 Cyber attacks are COVID related – UK NCSC

- Attacks were up 3x in April and 2x June over the previous year. –F5

- Malicious COVID Domains created by tens of thousands per day 90% are Scams according to ZDNET

- 2,000% increase in malicious files with "Zoom" in the name.

- The #3 most worrisome fallout of a prolonged Pandemic is an increase in cyber attacks and data fraud. - WEF

- The rapid deployment of tech assets has increased cyber risk.

"How Cyber Attacks Changed During the Pandemic"

Incidents reported to the SIRT in 2020
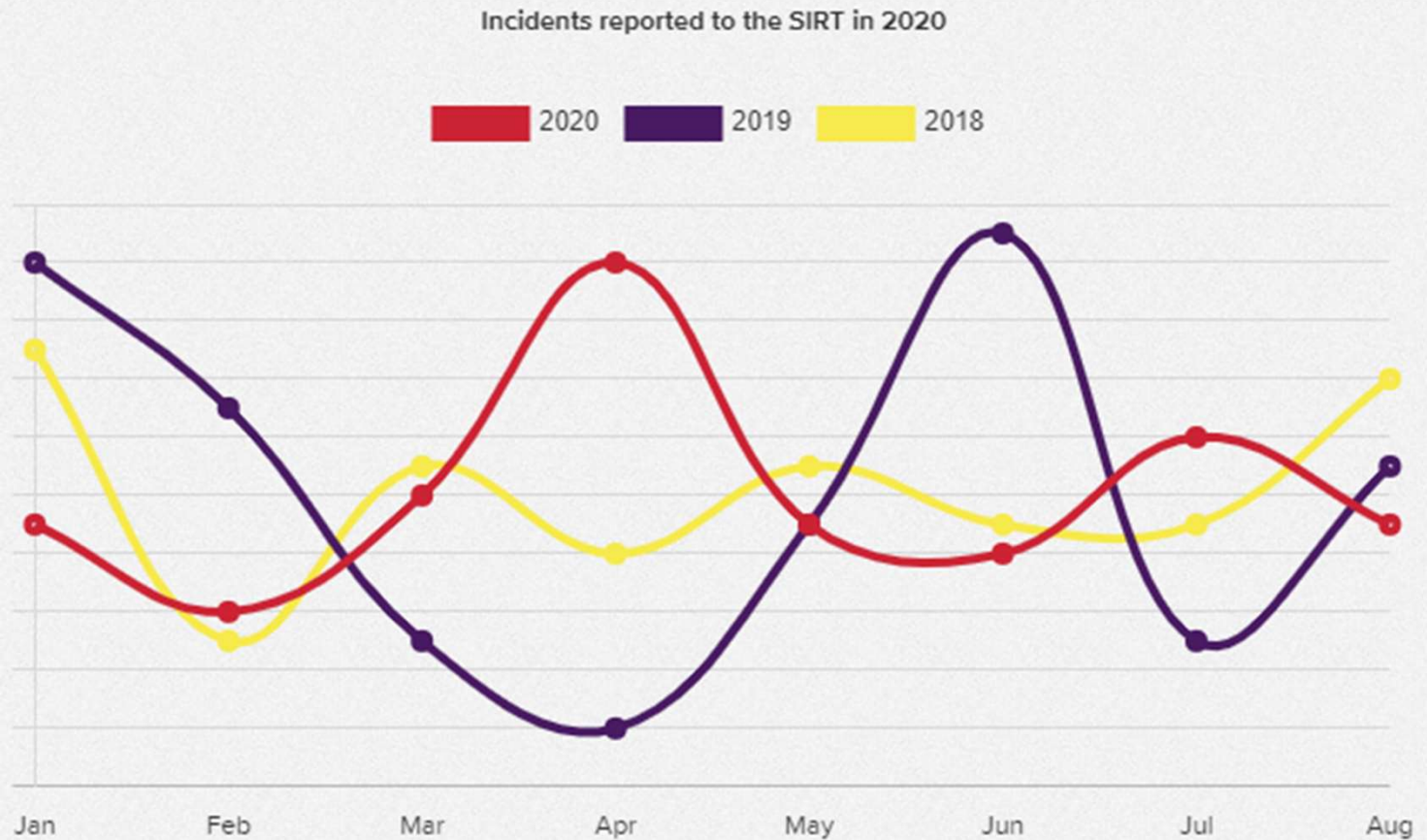
2020   2019   2018

Figure 1. Security incidents reported to the F5 SIRT from January through August for 2018-2020.

slido

What do you believe is your greatest Cyber risk during this Pandemic?

ⓘ Start presenting to display the poll results on this slide.

Increasing Threat Surface

- Patch management challenges

- Security protections at home.

- Apps

- Trusting Email over personal interaction

- Asset Management

D∅LL Technologies

Mitigating Cyber Events

People

- Education
  - How to recognize Phishing
  - What to do if you think a message is phishing
  - Cyber threats to your industry
  - Check for Updates

- Phishing Campaigns

- Educate User

- Educate Admin

- Educate Boards

- Educate Everyone

Processes

- Resilient Infrastructure

- What to do when _____?

- Center for Internet Security top 20

- Risk Management Frameworks

- Zero Trust

Technology / Resilient Infrastructure

- Patch management

- Backups

- Firewalls

- Malware Defense

- DNS Protection

- Two-Factor Authentication

- Professional Support

- Flight Recorder

DELLTechnologies

slido

How many Compliance and Security Frameworks are you required to abide by?

ⓘ Start presenting to display the poll results on this slide.

Risk, Compliance, and Security Frameworks

- RMF! Risk management framework NIST National Institute of Standards and Technology (https://www.nist.gov/topics/cybersecurity)

- CIS Controls Center for Internet Security Controls (https://www.cisecurity.org/controls/)

- ISO International Standards Organization ISO/IEC 27001 (https://www.iso.org/isoiec-27001-information-security.html)

- HIPAA Health Insurance Portability and Accountability ACT (https://www.hhs.gov/hipaa/index.html)

- PCI-DSS Payment Card Industry Data Security Standard (https://www.pcisecuritystandards.org/)

- GDPR General Data Protection Regulation (https://gdpr.eu/)

- CCPA California Consumer Privacy Act (https://oag.ca.gov/privacy/ccpa)

- SOX Sarbanes Oxley (https://www.sarbanes-oxley-101.com/)

- NERC CIP North American Electric Reliability Corporation Critical Infrastructure Protection (https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx)

- COBIT Control Objectives for Information and Related Technologies (https://www.isaca.org/resources/cobit)

- GLBA Gramm-Leach-Bliley Act (https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)

- FISMA FEDERAL INFORMATION SECURITY MODERNIZATION ACT (https://www.cisa.gov/federal-information-security-modernization-act)

- FedRAMP Federal Risk and Authorization Management Program (https://www.fedramp.gov/)

- FERPA Family Educational Rights and Privacy Act (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

- ITAR International Traffic in Arms Regulations (https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing)

- COPPA Children's Online Privacy Protection Rule (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule)

DELLTechnologies

Cost of a Cyber Breach

- Real Cost (avg cost in 2020 $3.86M per event)
  - Heath care up 10.5%
  - Energy up 14%
  - Retail up 9.2%

- Reputation Cost
  - Lost opportunity do to breach
  - Lost customer base do to bad publicity

slido

Do you think your Board is?

ⓘ Start presenting to display the poll results on this slide.

Board Room Discussions

For the Board

- CIOs and CISOs Educate

- Are you aware that we have to comply with the following___? What is the "so what"?.

- Cyber is both an opportunity and a business risk

- How do you want cyber threats communicated

From the Board

- How are we evaluating our Cyber Security Posture

- To what are we measuring our Cyber Protection by

- What is risk vs what our cyber insurance covers

- Given our Risk, what are our reporting requirements

DELLTechnologies

References

- https://www.zdnet.com/article/cybersecurity-one-in-three-attacks-are-coronavirus-related/
- https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
- https://www.zdnet.com/article/cybersecurity-one-in-three-attacks-are-coronavirus-related/
- https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/
- https://www.cisecurity.org/blog/cybersecurity-challenges-of-a-remote-workforce/
- https://www.f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic
- http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf
- **https://www.sciencealert.com/viral-russian-app-that-makes-you-look-old-is-probably-keeping-your-data**
- **https://unit42.paloaltonetworks.com/covid19-cyber-threats/**
- **https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html**

DELL Technologies