Cybercrime: COVID-19 IMPACT & Auditing Considerations

Presented by:
Antonina K. McAvoy and Ryan L. Davis
PBMares Cyber & Control Risk Services

Certified Public Accountants & Consultants

Current State We Live In

PBMares SM

Image Source: AFP 2019

Image Source: Realnoe Vremya 2018

Global Cyber Warfare

PBMares

AMERICAS

- A sharp increase in COVID-19 themed phishing and fraud campaigns that leverage the coronavirus crisis and the subsequent lockdown were reported by respondents.
- As many companies in the Americas implemented teleworking, cybercriminals are increasingly targeting employees in order to gain control through remote access to corporate networks with a view to stealing sensitive information.
- A ransomware campaign carried out mainly through LOCKBIT malware is currently affecting medium-sized companies in some countries within this region.
- Social media is increasingly used by criminals for online child sexual exploitation. Specifically, offenders within online child abuse networks are locating and contacting their victims on social media taking advantage of the global lockdown. At the same time, the trade in child sexual exploitation images has intensified.

Image Source: Interpol 2020

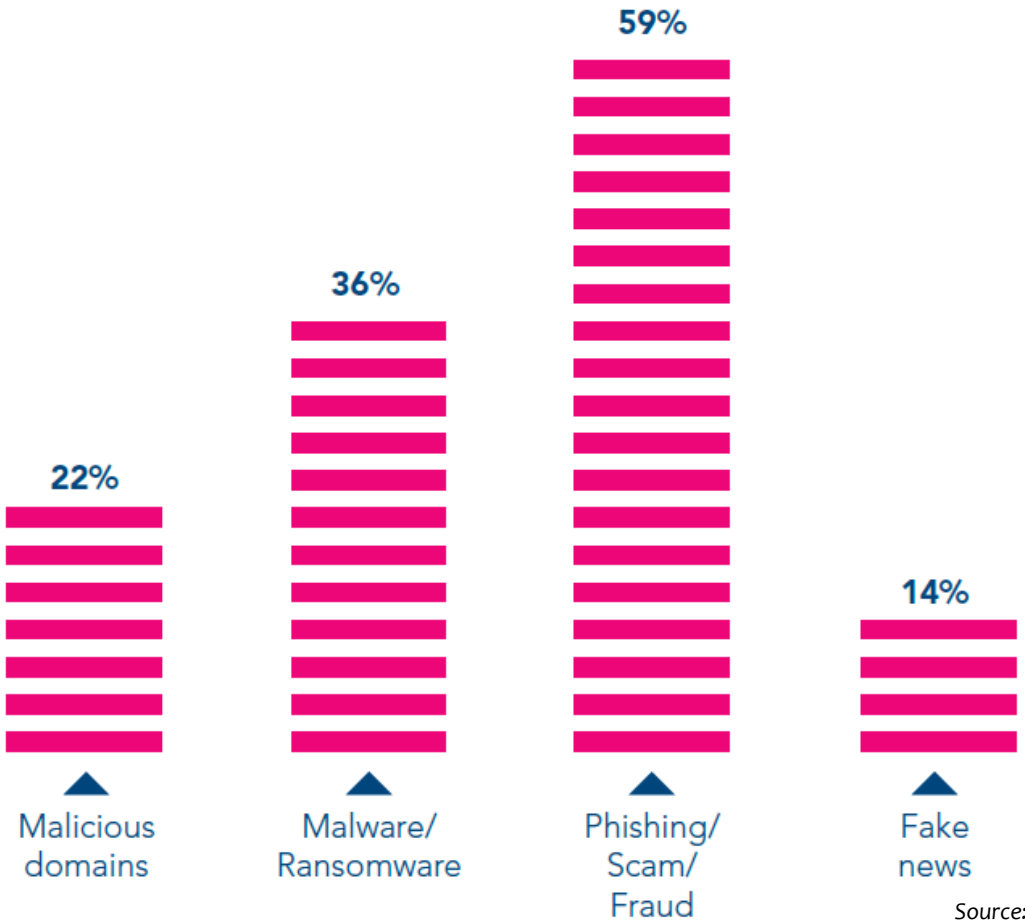
Image Source: Microsoft 2020

Key COVID-19 Cyber Threats

PBMares

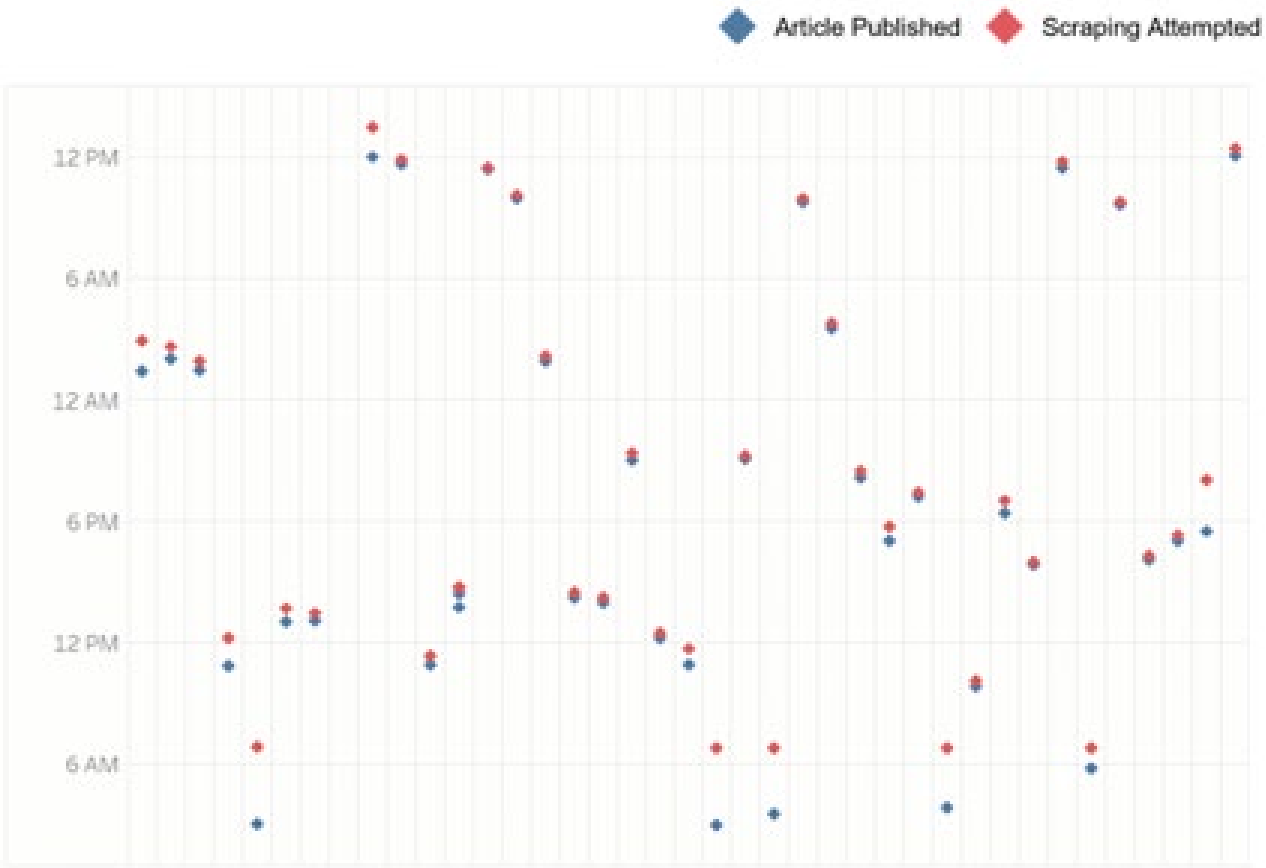
EVOLUTION OF CYBER WARFARE

Image Source: OODA 2020



Source: Interpol 2020

Bots - *A Dangerous Internet Threat*



Virus Concerns Used to Trick

PBMares

JOHNS HOPKINS UNIVERSITY & MEDICINE | CORONAVIRUS RESOURCE CENTER

Home | Tracking | Testing | Tracing | By Region | News & Resources | About

Tracking Home | Critical Trends | Global Map | U.S. Map | Data in Motion

COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

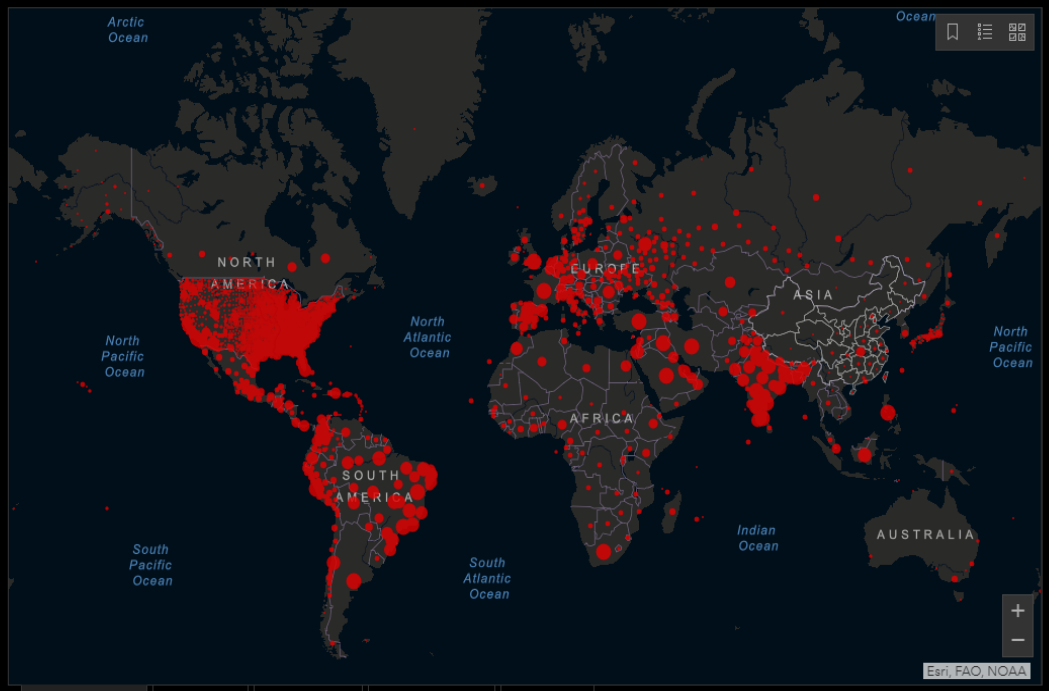
Global Cases
34,103,279

Cases by Country/Region/Sovereignty

- 7,255,546 US
- 6,312,584 India
- 4,810,935 Brazil
- 1,179,634 Russia
- 829,679 Colombia
- 814,829 Peru
- 778,607 Spain
- 751,001 Argentina
- 743,216 Mexico
- 674,339 South Africa
- 616,960 France
- 464,750 Chile
- 462,774 United Kingdom
- 461,044 Iran
- 367,474 Iraq
- 364,987 Bangladesh

Admin0 | Admin1 | Admin2

Last Updated at (M/D/YYYY)
10/1/2020, 2:23 PM



Cumulative Cases | Active Cases | Incidence Rate | Case-Fatality Ratio | Testing Rate

188
countries/regions

Lancet Inf Dis Article: Here. Mobile Version: Here. Data sources: Full list. Downloadable database: GitHub, Feature Layer. Lead by JHU CSSE. Technical Support: Esri Living Atlas team and JHU APL. Financial Support: JHU, NSF, Bloomberg Philanthropies and Stavros Niarchos Foundation. Resource support: Slack, Github and AWS. Click *here* to **donate** to the CSSE dashboard team, and other JHU COVID-19 Research Efforts. FAQ. Read more in this blog. Contact US.

Global Deaths
1,016,167

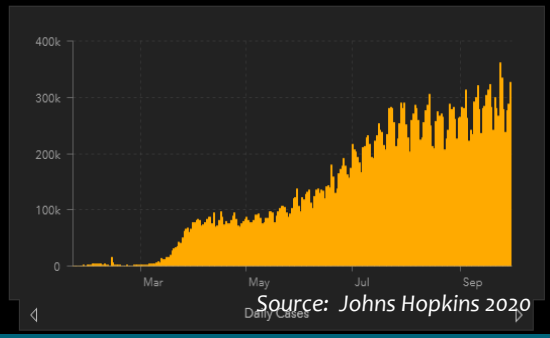
- 207,374 deaths US
- 143,952 deaths Brazil
- 98,678 deaths India
- 77,646 deaths Mexico
- 42,292 deaths United Kingdom
- 35,918 deaths Italy
- 32,463 deaths Peru

Global Deaths | Global Recovered

US State Level
Deaths, Recovered

- 33,159 deaths, 76,754 recovered New York US
- 16,140 deaths, 34,859 recovered New Jersey US
- 16,026 deaths, 664,883 recovered Texas US
- 15,917 deaths, recovered California US
- 14,444 deaths, recovered Florida US
- 9,456 deaths, 113,768 recovered Massachusetts US
- 8,940 deaths, recovered Illinois US

US Deaths, Recovered



Source: Johns Hopkins 2020

Data Is The New Oil

PBMares

Polling Question #1

Question: Do you maintain a current listing of all information systems where sensitive information resides?

A) Yes – it has been updated in the last 6 months
B) Yes – but it has not been updated in over 1 year
C) No – we have not done a data mapping

Remote Workers

PBMares

PRE COVID-19 COMPARISON

Remote work challenges for credit unions

- Communicating organizational culture
- Facilities management
- Technology and cybersecurity
- Health and safety
- Ensuring continued productivity

Source: American Banker 2020

9.8 Million → 65.9 Million Remote Workers

Remote Worker Attack Vectors

PBMares

Fraudulent Website Login Pages

Virtual Private Network (VPN)

Advanced Persistent Threat (APT) Attacks

Cloud Vulnerabilities

Social Engineering Attacks

Videoconferencing

E-mail Malware Phishing Campaigns & E-mail Fraud

Image Source: UHWO Cyber 2020

COVID-19 Fraud Schemes

PBMares

CREDIT UNIONS & OTHER FINANCIAL INSTITUTIONS

New Account Fraud

Identity Theft

Imposter & Money Mule Schemes

Cybersecurity Risks

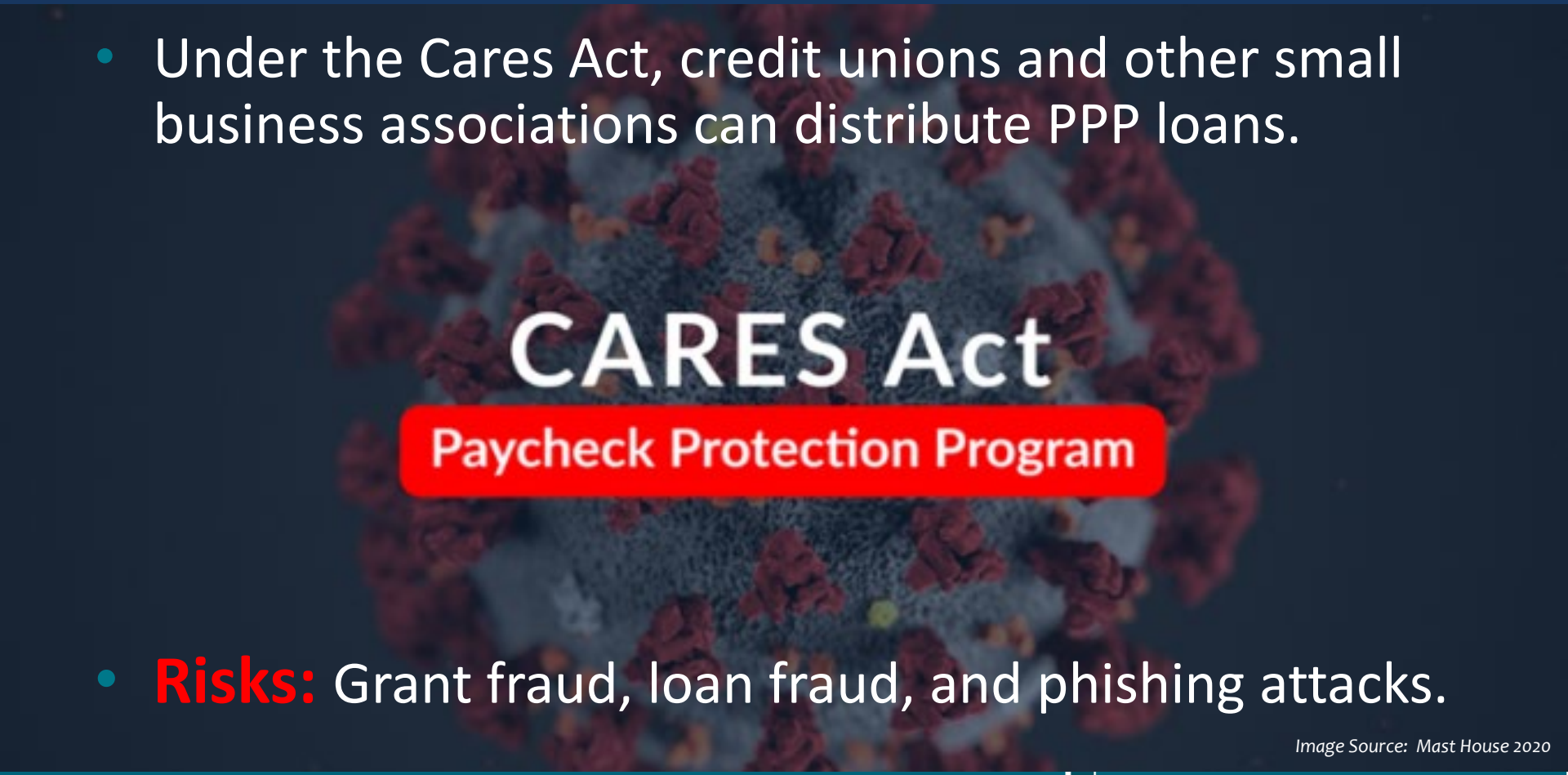
Mobile Banking Application Fraud

Example: COVID Fraud Scheme

PBMares

IN THE NEWS

- Under the Cares Act, credit unions and other small business associations can distribute PPP loans.



- **Risks:** Grant fraud, loan fraud, and phishing attacks.

Image Source: Mast House 2020

COVID-19 Social Engineering

PBMares

- Demand for accurate information on the crisis.
- Deepened online dependence.
- Expanded use of email and social media.
- Sudden mandate to work from home.
- More vulnerable economic situations.
- Community efforts to mitigate pandemic risks.

Phishing

PBMares

SOCIAL ENGINEERING

From:
Date: Monday, 2
To: "noreply@co
Subject: See Cov

Dear Customer,

Hope this email fir
As part of promise
confirmation page

PDF Promocode_f

This should be cre

Regards

payment

Latest on corona-virus - Message (HTML)

File Message Tell me what you want to do...

World Health Organization: WHO <[redacted]>

Latest on corona-virus

This message was sent with High importance.

MBET

MyHealth-Ebook.zip
22 KB

World Health Organization

Corona-virus updates

Concerning Corona-virus disease (COVID-19) outbreak, the World Health Organization brings you the Corona-virus E-Book and Guide.

Inside this E-Book (**My-health**), you shall find out the complete research/origin of corona-virus and the recommended guide to follow to protect yourself and others.

Guidance to protect children and business centre;

This guidance provides critical considerations and practical checklists to keep Kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.

Critical preparedness, readiness and response actions for COVID-19;

Malicious Websites

PBMares

TARGETED ATTACKS THROUGH SPOOFED COVID-19 RELIEF WEBPAGES

Small Business Admini | Login - SBA Economic In

https://leanproconsulting.com.br/gov/covid19relief/sba.gov/

MALICIOUS URL

SBA U.S. Small Business Administration

CREDENTIAL THEFT

Sign in to Your Account

Access your SBA Economic Injury Disaster Loan Portal Account to review your application and track your loan status.

Username or email

username or email

Password

password

Remember username/email

Forgot your password?

Sign in

Questions? Call 1-800-659-2955 | TTY/TDD: 1-800-877-8339

Monday - Sunday, 8 a.m. - 8 p.m. ET

Business Email Compromise

PBMares

SOCIAL ENGINEERING

INTERPOL

THE ANATOMY OF BUSINESS EMAIL COMPROMISE

3 TOXIC INGREDIENTS

Low cost!
Low risk!
High rate of return!

= **Millions in illegal profits**

Hacking
An email account is compromised through malware, employee intrusion, etc.

Social engineering fraud
The victim is manipulated into providing information or funds.

Money laundering
Multiple transfers are made involving foreign banks/ institutions

#BECareful

Image Source: Interpol 2020

Financial Malware

PBMares

BANKING TROJANS

- **Trojan Name:** Dridex (one of the most prevalent financial Trojans).
- **Primary distribution**: phishing e-mail spam campaigns
- **Risk:** Impacts confidentiality of customer data and availability of data and systems for business processes.

Videoconferencing

PBMares

CYBER REMOTE WORK THREATS

Source: Palo Alto 2020

Ransomware

PBMares

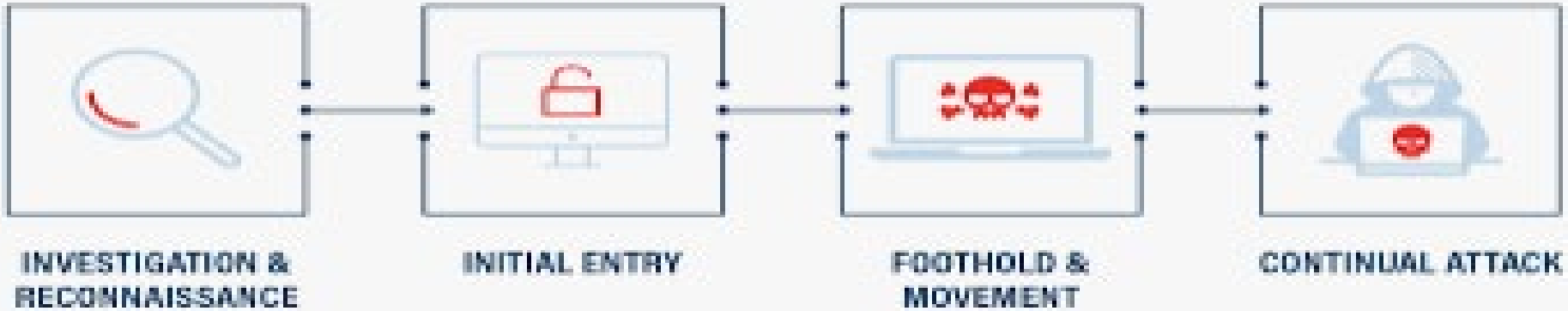
CYBER REMOTE WORK THREATS

- Monitoring
- Backups
- Access

Advanced Persistent Threat (APT)

PBMares

CYBER REMOTE WORK THREATS

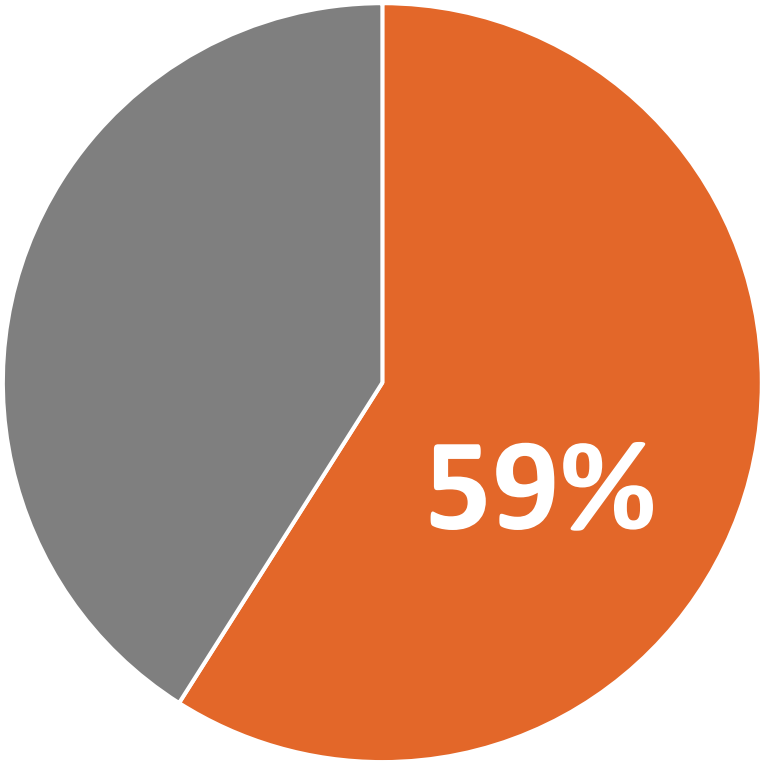


Third-Party Vendor Risk

PBMares

DATA BREACHES CAUSED BY A THIRD-PARTY VENDOR

PONEMON INSTITUTE



- Polling Question #2

  Question: What do you see as the biggest challenge your organization faces in managing cyber risks during the COVID-19 pandemic?

  A) Security Awareness Training
  B) Updated Cyber Risk Assessment
  C) Updated InfoSec Policies and Procedures
  D) Mapping where our data lives and how it is protected

Cyber Risk Management

PBMares

Top 8 Things to Improve Cybersecurity for a Remote Workforce

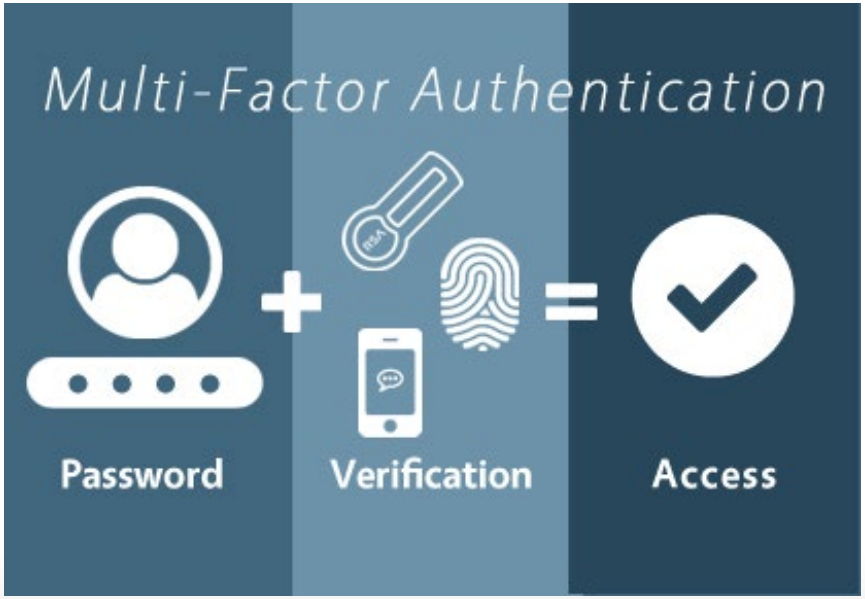
1. Utilize a Virtual Private Network (VPN)

- Keep employees secure with your enterprise security suite
- Use always on VPN connections, if possible

Top 8 Things to Improve Cybersecurity for a Remote Workforce

2. Enable Multi-Factor Authentication

- Additional layer of protection for accessing your most important resources



Top 8 Things to Improve Cybersecurity for a Remote Workforce

PBMares

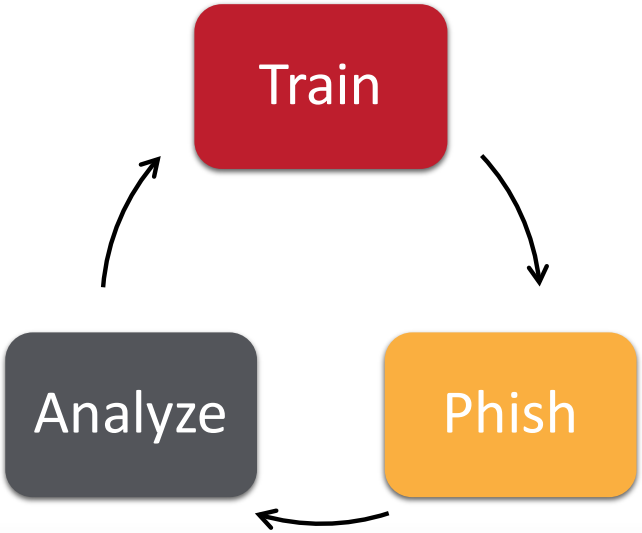
3. Ensure Software is Current

- Operating Systems
- Third-party applications
- Anti-virus and anti-malware solutions

Top 8 Things to Improve Cybersecurity for a Remote Workforce

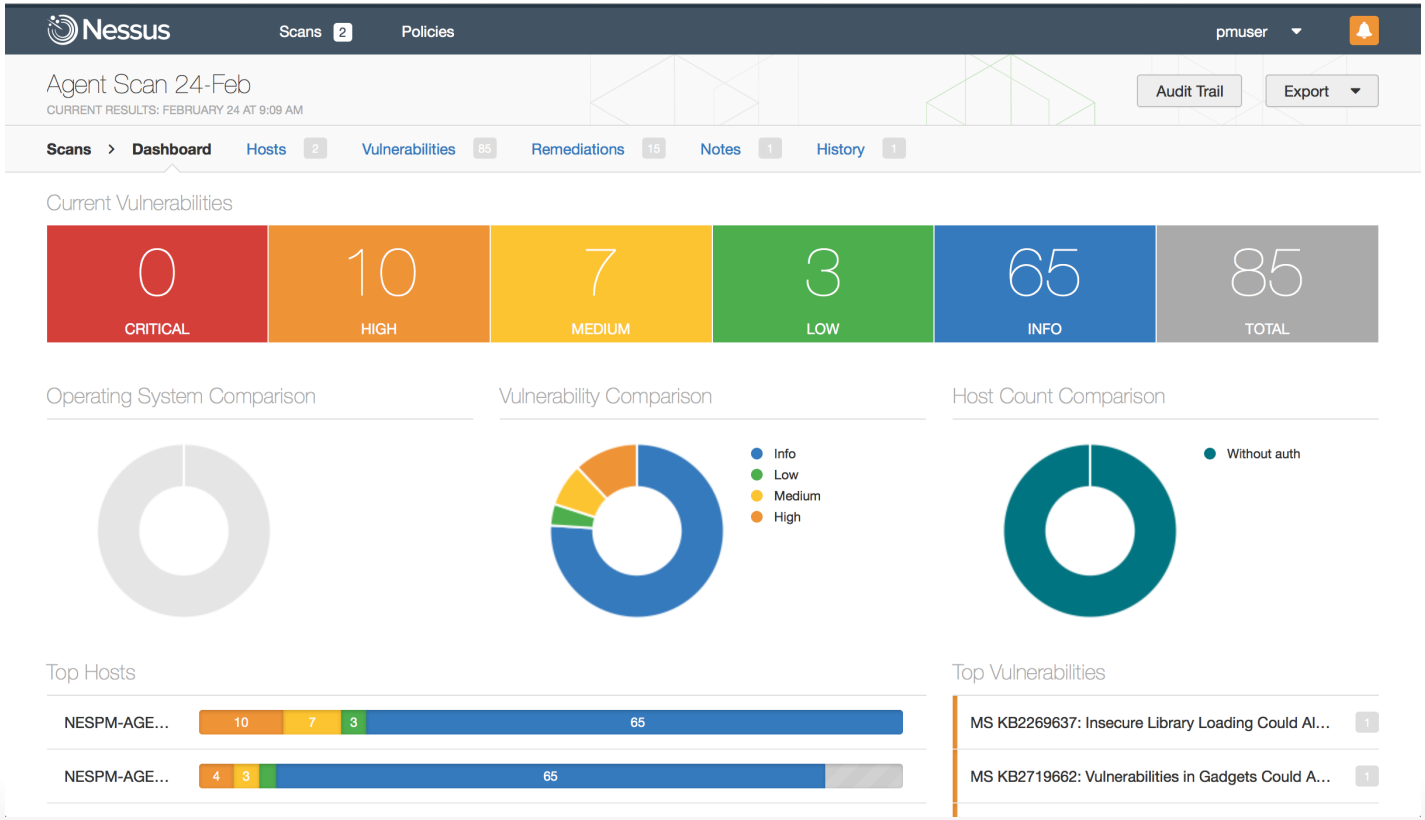
4. Security Awareness Training

- While your employees are your greatest asset…**95% *of all cyberattacks are caused by*** *human error…*



Top 8 Things to Improve Cybersecurity for a Remote Workforce

5. Vulnerability Scans



Top 8 Things to Improve Cybersecurity for a Remote Workforce

PBMares

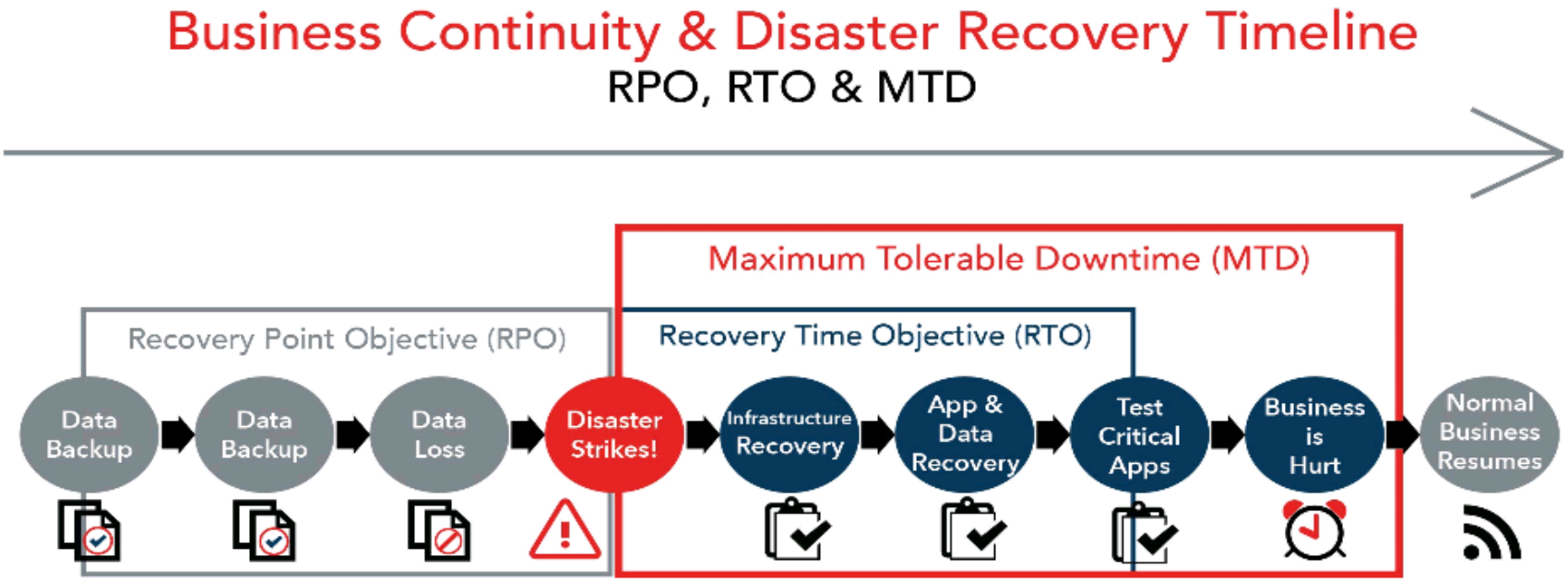
6. Incident Response

- Ensure employees are educated on what to do when they suspect a security incident
  - Disconnect the device from the internet
  - Keep the computer on to preserve forensic evidence
  - Report the incident immediately

Top 8 Things to Improve Cybersecurity for a Remote Workforce

7. Business Continuity Planning

"Plan for the worst, hope for the best"



Polling Question #3

How adequate was your organization's Continuity Plans (Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan) in helping your organization navigate the COVID-19 crisis?

A) **Exceptional:** there were no major issues
B) **Fair:** there were minor issues but we overcame them quickly
C) **Poor:** we faced significant challenges
D) **Unacceptable:** we have not been able to adapt to these circumstances

Top 8 Things to Improve Cybersecurity for a Remote Workforce

6. Proper Cyber Insurance Coverage

Audit Considerations (1 of 4)

PBMares

STRENGTHEN SECURITY POSTURE

Verify employees/contractors received cyber awareness training.

Verify a formally documented/up-to-date IT risk assessment exists.

Verify continuity plans are up to date and table top exercises are performed annually: Incident Response Plan, Business Continuity Plan, and Disaster Recovery Plan.

Verify passwords and multi-factor authentication.

Audit Considerations (2 of 4)

PBMares

STRENGTHEN SECURITY POSTURE

Require verification.

Require e-mail signing signatures.

Verify spam filters are enabled and block all access to suspicious or blacklisted websites.

Verify anti-virus, firewall, and other tools that scan computers and devices regularly to prevent malware infections are up-to-date and configured properly.

Audit Considerations (3 of 4)

PBMares

STRENGTHEN SECURITY POSTURE

Require warning banners for all emails external to the organization.

Verify systems have the latest security updates.

Verify file and printer sharing services are disabled. If services are required, use strong passwords / AD authentication.

Verify user permissions to install and run unwanted software applications are restricted.

Audit Considerations (4 of 4)

PBMares

STRENGTHEN SECURITY POSTURE

Verify strong password policy across all technology layers.

Verify all software/USBs are scanned prior to executing.

Verify vulnerability scanning and penetration testing is performed regularly, and high/critical risks are remediated timely.

Verify operating system patches are up to date.

About PBMares
Cyber & Control Risk Services

PBMares

- PBMares has been specializing in IT and Cyber Security auditing for more than 15 years. Service include:
  - Attestation
    - IT General Controls Audits (ITGC)
    - Service Organization Control (SOC) Audits – SOC1, SOC2, SOC3 & SOC for Supply Chain
  - Consulting
    - DFARS, CMMC, HIPAA, and Cyber Risk Assessments
    - Review of Cyber Insurance Coverage
    - Vulnerability Scans of Network (Internal and External)
    - Penetration Testing
    - Incident Response Consulting
    - Data Classification Process Design and Consulting
    - Review and Development of Information Security Program Policies and Procedures
    - Information Security Awareness Training
    - User Life Cycle Management Consulting

Contact

Antonina K. McAvoy, CISA
Manager, Cyber & Control Risk Services

150 Boush Street, Suite 400
Norfolk, VA 23510
Phone: (757) 355-6011
amcavoy@pbmares.com

Visit **www.pbmares.com** to read our blog and learn of upcoming events.

Contact

Ryan Davis
Senior, Cyber & Control Risk Services

150 Boush Street, Suite 400
Norfolk, VA 23510
Phone: (757) 355-6011
amcavoy@pbmares.com

Visit **www.pbmares.com** to read our blog and learn of upcoming events.