RGP
To the Power of Human™

Presentation to the ISACA South Florida Chapter

Cybersecurity Audits: What We Learned in a 2020 Remote Work Environment

January 13, 2021

Lynn Rohland
Vice President, Risk & Compliance
Cybersecurity & Data Privacy Practice Lead

Agenda

- Work Environments Pre-COVID
- Pandemic Impact on IT Depts.
- Cyber Threat Landscape
- 2020 Audit Findings & Themes
- 2021 Audit Plan Considerations
- Wrap-Up and Q&A

Pre-COVID, the adoption of remote work-enabling technologies and environments were on the rise.

2019 Global State of Remote Work Report, found 62% of U.S. workers had some type of telework arrangement – even if once a month or when needed.

The same report found 48% of those polled worked remotely at least once per week.

Buffer's 2019 Remote Work Report revealed of the 2,500 employees surveyed, that 98% seek some type of remote arrangement for the rest of their career.

2019 Owl Lab Survey

2019 Survey by Buffer

Pandemic Impact on IT

Pandemic forced businesses to reform many of their IT operations.

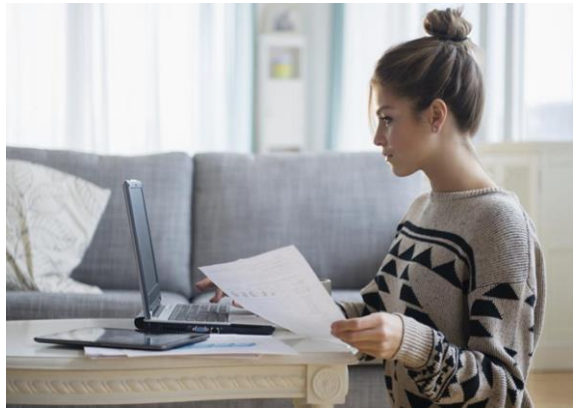
- Demands on networks, bandwidth and infrastructures imploded.
- Although IT investments were on the rise, COVID caused a scramble for new technologies to enable business continuity.
- IT infrastructures now also had to support remote workforces.
- Oct. 2020 survey of executives revealed a 3-4 year acceleration of digitizing customer and supply-chain IT interactions.
- The criticality of strengthening cybersecurity strategies ensued; and priorities on IT governance and data protection increased.
- Within weeks of the WHO declaring a pandemic, it reported a five-fold increase in cyber-attacks itself on its own systems.

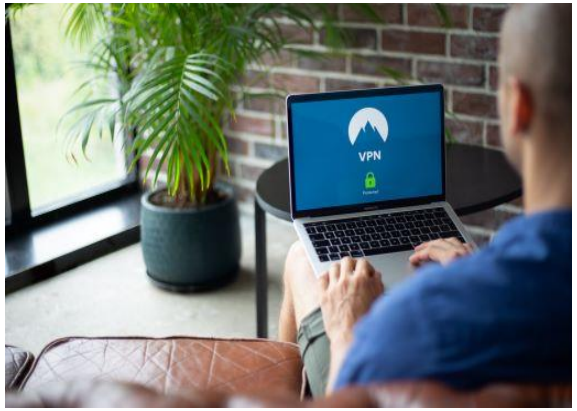
Polling Question: #1

How many organizations have already finalized their 2021 Audit Plans?

Cyber Threat Landscape

The largest remote workforce in history resulted in the greatest threat landscape for businesses.





- No need to conjure up new tactics as COVID-19 provides them with a greater attack surface.
- Malicious hackers are now attacking computers and networks at a rate of every 39 seconds (U of Md.).
- Q1 of 2020 showed a 600% spike in email phishing attacks.
- Phishing attacks subsequently led to an uptick in ransomware attacks by 139%.
- Ransomware attacks against healthcare providers are becoming more prevalent.
- Finally, 1 in 3 companies paid the ransom price averaging $110K in Q1 to $170K in Q3.

2020 Remote Work Audit Findings & Themes

2020 audit plans revised to include cyber and remote work.

RGP™

Hospitality Sector –

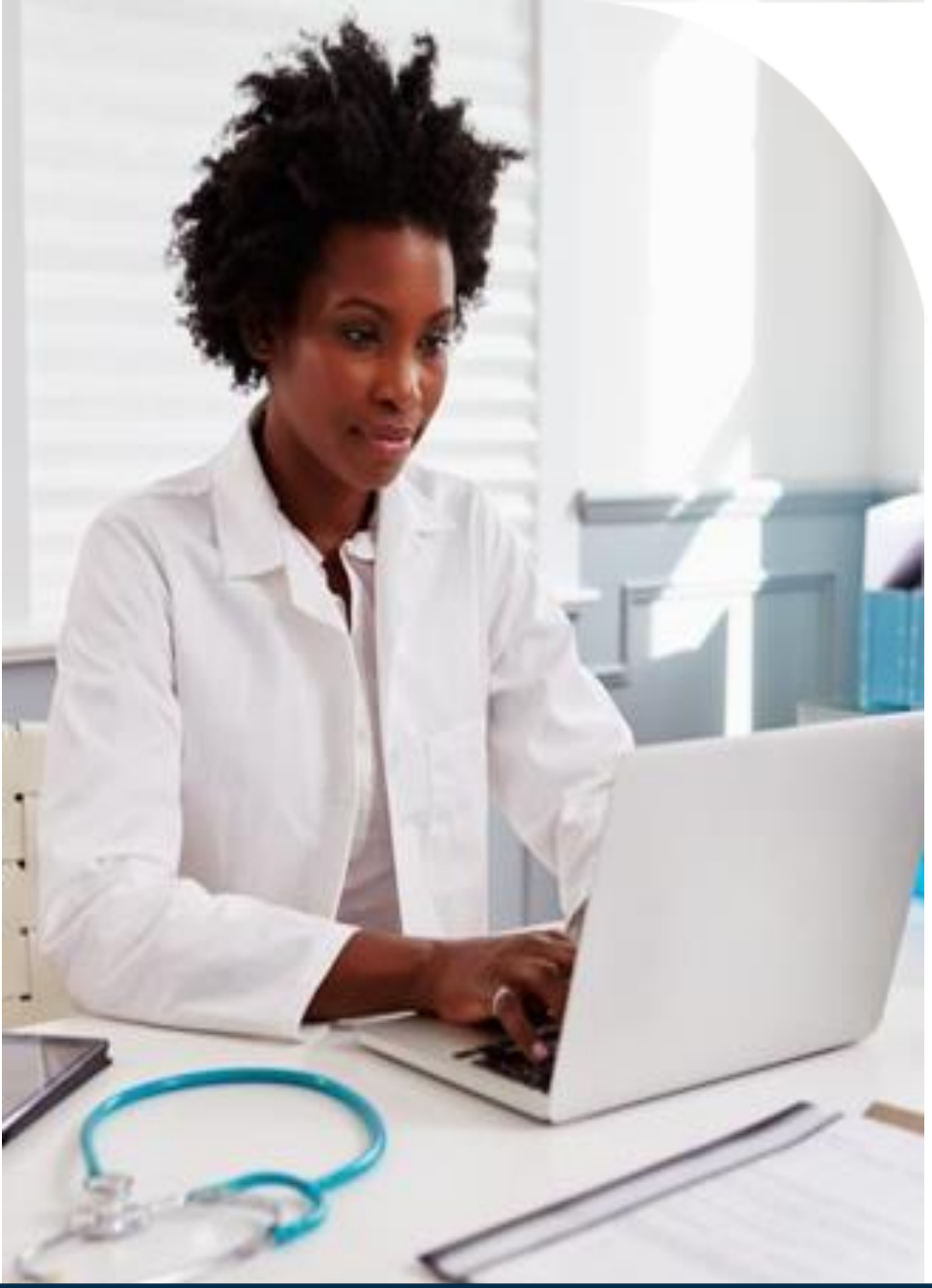
1. Lack of control owners identified for IT security and application controls.
2. Lack of documented procedures and processes for newer applications.

Cause: COVID-19 severely impacted the leisure and travel sector, resulting in workforce reductions impacting IT Depts. And thus, historical knowledge and accountability.

Finance Sector –

1. Lack of controls designed to help mitigate reoccurring data incidents.
2. Lack of training for role-based positions – some required by law.

Cause: Lack of design and operational effectiveness of controls for handling of personal information. Lack of mapping risk controls to cybersecurity laws and privacy regulations. Accountability decentralized and diluted across enterprise.



2020 audit plans (cont'd)

Retail Sector –

1. Lack of policies and procedures for identity and access management.
2. Delayed adoption of the IAM platform solution in place.

Cause: Company was actively interviewing a half dozen IT security vacancies when shelter-in-place hit, affecting retail stores that resulted in hiring freezes. Thus, a shortage of IT security employees to move IT roadmaps forward.

Healthcare Sector –

1. Lack of standards and procedures for periodic review/handling of third-party and vendor access credentials.
2. Lack of effective IT security and data privacy training.

Cause: Quantity of vendors providing outsourced or specialty services, and back-office solutions is expansive and remains a struggle for many. While training at or near 100% completion by employees, its effectiveness fell short.

2020 audit plans (cont'd)

Additional observations noted:

- Remote work policies and processes outdated or drafted in a rush.
- Training and IT security expectations overlooked for remote workers.
- BCPs not properly established or adequately stress-tested.
- Lack of software inventory of IS and application assets.
- Lack of visibility into mapping of internal controls to regulations.
- Lack of controlled use of admin privileges and segregation of duties.
- Lack of a periodic review of third-party and vendors accounts with remote access to information systems and data.
- Lack of data inventories.

Polling Question: #2

Do you anticipate 50% or more of your organization's current remote employees to remain remote throughout 2021?

2021 Audit Plan Considerations

2021 Audit Plan considerations focus on the trends, threats, and emerging issues.

The severity of the cybersecurity landscape continues to escalate due to:

- Cybercriminals attempting network attacks every 39 seconds,
- Global pandemic causing a seismic shift in how we deliver products and services,
- Shelter-in-place reshaping work environments to mostly a remote workforce,
- And now, the discovery of the largest, state-sponsored cyberattack on the United States' critical infrastructure and federal departments,

These trends and events influence what businesses decide to include in audit plans this year – from evaluating an organization's readiness in response to these developments, to testing the effective management of the impact from these disrupters.

World-wide response to COVID-19 reshaped many Ops forever … remote working is here to stay.

- Nearly 70% of US employees now working from home full-time.
- 75% state they're equally or more productive working remote.
- Video meetings up by 50% since pre-pandemic.
- 80% expect to work from home at least 3x/wk.

2020 Owl Lab Survey

2020 Survey by Buffer

- 25% of respondents report working *more* hours.
- 20-25% of companies pay or share home office costs.
- Employees saving avg. $479.20/mo. and businesses $11K per year, per employee
- 1 in 2 employees report not returning to job if it doesn't offer remote work options.

2021 Audit Plan considerations (cont'd).

1. Physical and Logical Access Controls
2. Hardware & Software Asset Inventories
3. Data Inventory Management
4. Mapping of Controls to Regulatory Mandates
5. CPRA (aka CCPA v2.0), GDPR, HIPAA Audits
6. Third-Party Risk Management
7. Patch Management
8. Stress-Testing BCP
9. Training. Training. And more Training
10. Adequate Staffing & Segregation of Duties

* Evaluation of Risk Culture

Gartner's 2021 Audit Plan Hot Spots Report

2021 Audit Plan Hot Spots

- IT Governance
- Data Governance
- Third-Party Management
- Cyber Vulnerabilities
- Business Continuity & Disaster Recovery
- Talent Resilience
- Corporate Responsibility
- Risk Culture & Decision Making

Polling Question: #3

Recap: 'Risk Culture' is a construct of values and behaviors present throughout an organization that shape day-to-day risk decisions.

How many of you have begun to integrate a Risk Culture across your 1st line of defense?

Wrap-Up / Q&A

Wrap-up & Key Takeaways:

RGP™

Audits should reflect the new landscape of risk, vulnerabilities and threats that we've seen trending in recent months:

- Understand areas of IT governance requiring greater scrutiny due to the rapid acceleration of technologies rolled out that enabled a largely remote workforce.
- Review third-party agreements and contracts for clearly defined IT security expectations and the processes to monitor their compliance.
- Consider evaluating how well training initiatives are working including whether individuals/specific roles are obtaining the necessary training.
- Determine how well the organization is mapping its controls not only to risk mitigation but also to regulatory and legal mandates.
- Consider how employees in the organization will report for work in 2021, and any lessons-learned from 2020 shelter-in-place.

Thank You,

Q&A

Lynn Rohland
Vice President, Risk & Compliance
Cybersecurity & Data Privacy Practice Lead
Lynn.Rohland@rgp.com
M: +1 703 801 6075

RGP
To the Power of Human™