Bressler
AMERY & ROSS

COVID-19:
Cybersecurity and Data Privacy Concerns in the Home Office

Presenters: David Butler, Brian Ellis, Marc Issa, Nikolas Komyati

Overview

TODAY'S DISCUSSION

- Update on key regulatory deadlines
- Notable statistics
- Lawyers working from home: Ethics and other concerns
- Telework Issues: VPNs, passwords, networks, secure Wi-Fi
- Enforcement of company/firm policies with employees working remotely

Update on Key Regulatory Deadlines

NYDFS 2019 Compliance Certification Filing Deadline Extended

- With respect to compliance with DFS's cybersecurity regulation (23 NYCRR 500)("Part 500"), DFS has extended the Compliance Certification Filing Deadline for Year 2019 from April 15, 2020 to June 1, 2020 due to the pandemic.
  - All Covered Entities and licensed individuals who are not fully exempt from Part 500 now have until June 1, 2020 to submit the required Certificate of Compliance, certifying their compliance for the 2019 calendar year.
  - Covered Entities do not need to file new Notices of Exemption. If there have been any changes from previous filings, then the entity or individual should update their status accordingly.

Cyber Scams and COVID-19

Phishing and Other Cyber Scams

1 in 50 URLs is malicious

Nearly 33% of phishing sites use “HTTPS” to appear secure and legitimate

Phishing for log-in credentials constitutes the majority of data breaches

9 in 10 encounters with malware stem from emails delivered to a business’s employees

Sources: Webroot Inc. “2019 Webroot Threat Report: Mid-Year Update.” (September 2019); Verizon. “2019 Data Breach Investigations Report.” (May 2019)

Data Breaches and the Workplace

More than two-thirds of workers are sure they have received a phishing email at work

Average total cost of a data breach is now nearly $4 million

35% of workers who ***know they have been hacked*** do not change their password

Nearly half of employees admit they click links from unknown senders at work

Sources: 2019 Hiscox Cyber Readiness Report; IBM. “2019 Cost of a Data Breach Report.” (July 2019); Webroot Inc. “Hook, Line, and Sinker: Why Phishing Attacks Work.” (September 2019)

COVID-19 Based Cyber Threats

- Now, cyber threat actors are seeking to capitalize on the global concern over the novel coronavirus, COVID-19.
- Coronavirus based phishing scams have arrived via malicious emails and compromised sites.

Coronavirus-themed domains are 50 percent more likely to be malicious than other domains

Over 4,000 coronavirus-related domains have been registered since January 2020

https://www.cyber.nj.gov/

COVID-19 and NJ

- The NJCCIC has noted an increase in COVID-19 cyber threats aimed at NJ state employees and the Garden State Network.

  - Eight of the ten top phishing campaigns in the past few weeks had COVID-19 lures

https://www.cyber.nj.gov/

Cyber Threats Identified

- Fake Johns Hopkins University COVID-19 live map
  - infects site visitors with the information-stealing AZORult trojan.

- Another phishing campaign included an .iso attachment that, when executed, delivers the GuLoader downloader, which downloads the LokiBot trojan.

- How are they spread?

https://www.cyber.nj.gov/

Avoid the Phishing Lures

- Do not click on links in unsolicited emails and be wary of email attachments.

- Do not reveal personal or financial information in emails, and do not respond to email solicitations for this information.

- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information.

https://www.cisa.gov/sites/default/files/publications/200306cisainsightsriskmanagementfornovelcoronavirus.pdf

Lawyers Working From Home

Ethics and Other Concerns

Lawyers Working from Home

Ethics and Other Concerns

- Comment 8 to Model Rule 1 makes clear, “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.”
- Clearly, the duty of competency requires cybersecurity considerations.

Ethical Concerns

- Inadvertent disclosure of client information. RPC 1.6 (c)
- Lawyer should protect against disclosure of client information.
- lawyers should take reasonable efforts to avoid data loss and detect cyber-intrusion.

Best Practices

Ethics and Other Concerns

- Lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach
  - ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 483 “Lawyers’ Obligations After an Electronic Data Breach or Cyberattack” (October 17, 2018).

Telework Issues and Recommendations

VPNs, Passwords, Networks, Secure Wi-Fi

Telework Policies

- As telework becomes prevalent, the Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity.
- Create a telework policy with defined scope, roles, responsibilities, eligibility.
- Must comply with Employment Laws/Firm Policies.
- Must meet requirements for physical and information security.

Use of Personal Devices

- **Organization-Owned vs Personal Devices:**
  - Secure access through personal devices
    - Mandatory Multi-factor Authentication (MFA) for remote access to any application, network, or service.
  - Implement controls to prevent downloading/storage to personal devices/ cloud.
  - Storage of Company/Client data must only be stored on Company Systems.

https://www.cyber.nj.gov/

VPNs and Secure Connections

- Remote work options—or telework—require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network.

https://www.us-cert.gov/ncas/alerts/aa20-073a

FINRA Guidance

FINRA guidance for Firms providing remote working access to employees:

- Train employees to connect securely to office applications from a remote location.
- Train employees about potential scams and other cyber attacks.
- IT should vet incoming calls - fraudsters may use the increase in remote work to engage in social engineering
  - Be aware of bogus calls requesting password resets or reporting lost phones or equipment.
- Employees should know relevant IT staff and contact them with any issues.

https://www.finra.org/rules-guidance/notices/information-notice-032620

Cybersecurity Considerations

- More vulnerabilities are being found in VPNs and targeted by malicious cyber actors.
- As VPNs are 24/7, organizations are less likely to keep them updated with the latest security updates and patches.
  - increased phishing emails targeting usernames and passwords.
- Organizations that do not use multi-factor authentication (MFA) for remote access are more susceptible to phishing attacks.
- Limited number of VPN connections can weaken cybersecurity.

https://www.us-cert.gov/ncas/alerts/aa20-073a

Enforcement of Company/Firm Policies

With Employees Working Remotely

Create Policy

Establish a work-from-home (WFH) policy:

- Scope: to whom does the policy apply?; when does the policy apply?
- Infrastructure: do employees have necessary equipment and software to work productively?
- Conditions: Consider daily calls or "check-ins" to ensure employees are focused and productive
- Compensation: Require tracking of time and activities on a daily basis as a requirement for compensation

Test Systems

- **Test your systems, policies, and employee understanding frequently to minimize business disruption.**
  - Document issues and resolutions
  - Consult with experts whenever necessary

Accountability is Key

- **Be accountable and require accountability.**
    - It is impossible to estimate the extent of disruption caused by remote work.
    - Teamwork is an essential ingredient to successfully developing, implementing, and using remote work capabilities.

Q&A

Who We Are

David Butler
Principal | New York
dbutler@bressler.com

Brian Ellis
Counsel | New Jersey
bellis@bressler.com

Marc Issa
Director of IT | New Jersey
missa@bressler.com

Nikolas Komyati
Principal | New Jersey
nkomyati@bressler.com

BIRMINGHAM, ALABAMA

2001 Park Place North • Suite 1500
Birmingham, AL 35203 • Phone: 205.719.0400

FORT LAUDERDALE, FLORIDA

200 East Las Olas Boulevard • Suite 1500
Fort Lauderdale, FL 33301 • Phone: 954.499.7979

MIAMI, FLORIDA

200 South Biscayne Boulevard • Suite 2401
Miami , FL 33131 • Phone: 305.501.5480

FLORHAM PARK, NEW JERSEY

325 Columbia Turnpike • Suite 301
Florham Park, NJ 07932 • Phone: 973.514.1200

NEW YORK, NEW YORK

17 State Street • 34th Floor
New York, NY 10004 • Phone: 212.425.9300

WASHINGTON, D.C.

1100 Connecticut Avenue • Suite 810
Washington, DC 20036 • Phone: 301.793.1370

Bressler
AMERY & ROSS