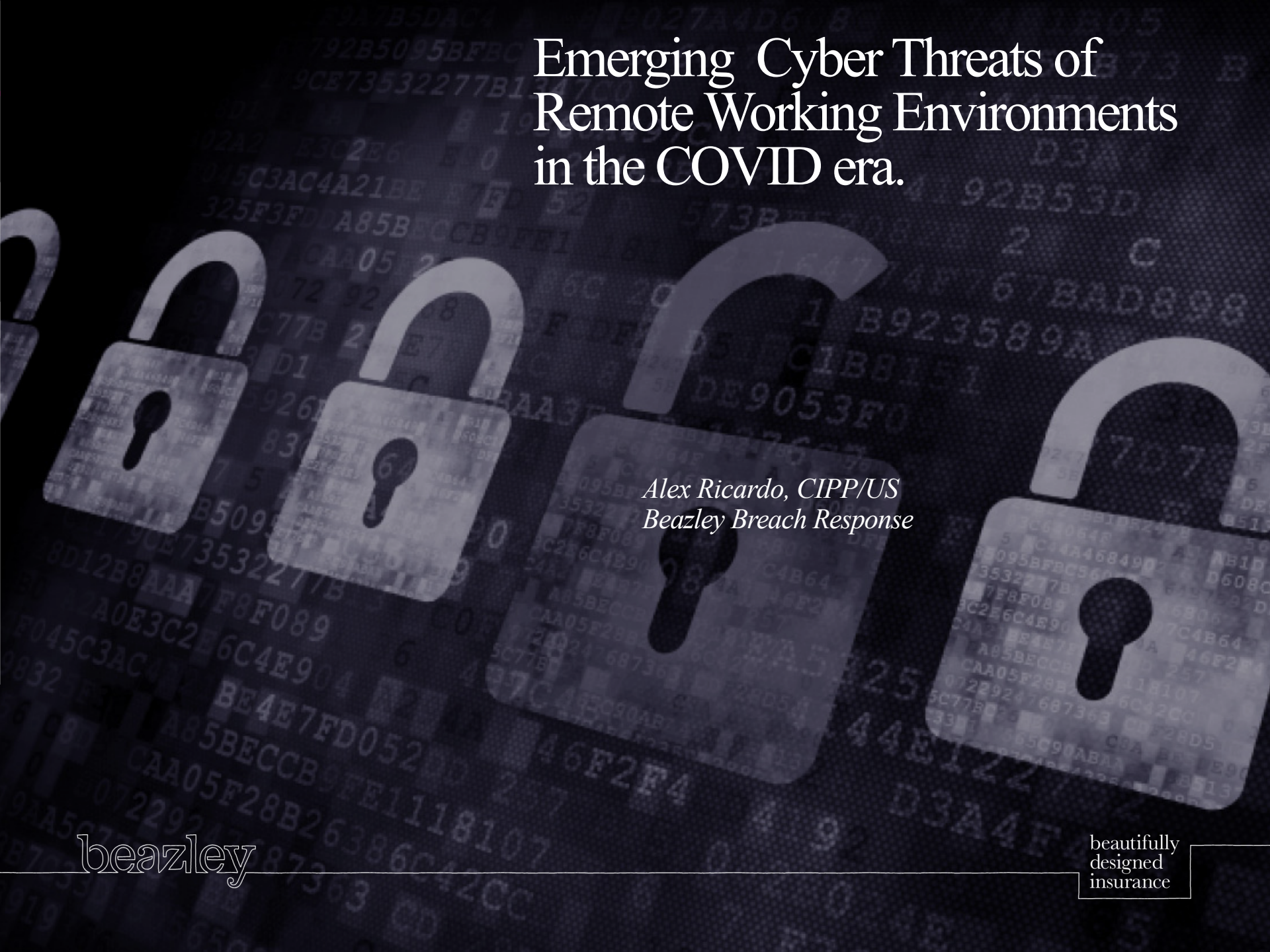
Emerging Cyber Threats of Remote Working Environments in the COVID era.



Alex Ricardo, CIPP/US
Beazley Breach Response

beazley

beautifully designed insurance

Disclaimer

This presentation and content is not meant to be considered professional legal advice.

The presenter is not a licensed attorney and all information obtained from this presentation should be considered for informational purposes only.

You should consult with a licensed privacy counsel for any decisions surrounding your corporate privacy initiatives, incident response plan or data breach response methodology.

Threat Landscape

beazley

High-Level Threat Landscape

Unintended Disclosure – Paper / Physical Records

- Shredding, Dumpster Diving, File Cabinets, Natural Disasters, Physical Social Engineering

Unintended Disclosure – Electronic Assets

- Computers, “Non-Computers”, Leased Equipment

Business Email Compromise

- 17% - ‘19 incidents (vs 24% - ‘18 incidents), “Red Letter Alerts”

Unencrypted Portable Devices

- 4% - ‘19 incidents (vs 24% - ‘17 incidents), Encrypt = 49 AGs “Go Away”

Broken Business Practices

- 17% - ’19 incidents

Rogue Employees

- 7% - ‘19 incidents, Disgruntled vs Enticed

COVID-era Threat Landscape

beazley

Work-From-Home Considerations in the COVID-era

- Shredders
- Home Wi-Fi
- VPNs
- Portable Device Usage (ie Thumb Drives)
- Printers
- BYOD (Bring Your Own Device)
  - Use of MDM (Mobile Device Management)
- Web Conference Services (Zoom / Webex)
- Rogue Employee – Enticed Activity

Ransomware

beazley

The cyber threat landscape is changing

Ransomware incidents

- 2015-2016 – "Turning Point" in Ransomware
- 20% (788) '19 incidents - 9% [(298) '18]
  - Healthcare, Financial Services, Professional Services, Manufacturing, Public Entities
  - Public Entities 13% of incidents (Q3-19) vs 3% (Q2-19)*
- SME vs MM – 62% vs 38% (2019) – Median company size: 62 employees
- Average Downtime – 15.0 Days *
- Remote Desktop Protocol (RDP) (aka Terminal Services) – still main attack vector *

* *Source: Coveware Q3 2019 Report*

Source: Beazley – 2018 statistics

Ransomware

" To 'B'reach Or Not To 'B'reach "

- Most are not breaches
- Forensics is necessary
  - Industry mandate may apply (ie: Covered Entities under HIPAA)
  - Retain under counsel
  - Need for regulatory inquiries in the future

Ransomware

Ransom Amounts

- $100s/$1000s/$10000s ► $100,000s/$1,000,000s
- Average Amount - $111,605* (33% increase from Q4-2019)
  - Actors are beginning to research financial viability and existence of cyber insurance to base amount*
- Beazley highest paid ransom – $7.5M
- Outliers are becoming more common and actors more bold
- Actors make up in volume
- FBI estimated in 2017, $1B were paid in ransomware demands

* *Source: Coveware Q3 2019 Report*

Ransomware

Who Are These Actors?

- No More 'Dark Hoodies'
  - Professional Business Model
  - "Best Customer Service"
- Bitcoin Wallet ID
  - "Double Dippers"
  - "Honor Amongst Thieves" – 99% odds of receiving encryption keys after ransom is paid
  - Known Terrorist Organizations

Ransomware

Why Would You Pay?

- "You Are Not the US Government"
- Technical Challenges at Data Restoration
  - Bad segmentation
  - Corrupt restored data
  - Improper backup intervals for data purpose
- 99% of companies received a working decryption tool if ransom was paid
  - Mamba has about 100% decryption recovery rate (DRR) with the decryption tool
  - Mr. Dec had a 30% DRR
  - Dharma/Phobos, Ryuk and Sodinokibi continue to dominate the ransomware market share
  - Average DRR – 96%

* *Source: Coveware Q3 2019 Report*

Ransomware

Who Do Actors Target?

- All industries targeted
- LinkedIn is their friend

Ransomware's Primary Attack Vector: RDP/RDG

beazley

Why is RDP and RDG an Emerging Threat?

- Primary Attack Vector for Ransomware hackers since 2018
- COVID-era related increase in employees remotely working from home have increased usage of RDP and RDG by corporations
- Employees “getting around” IT may not be versed in configuring RDP or RDG correctly.
    - Research and Development Departments
        - Higher Education
        - Research Healthcare Facilities

Remote Desktop Protocol (RDP)

What is RDP?

- Remote Access Tool for Microsoft Windows systems. (Interface to allow a user to connect to another computer over a network connection)
- Microsoft includes RDP functionality with all supported versions of Windows Operating System. Therefore, widely used and relatively easy to use with no additional configuration for use.
- Once enabled and reachable from the public internet, RDP is a "virtual open door". *Therefore, additional safeguards need to be implemented*.

Best Practices at using RDP

- Disable RDP altogether if you do not need or use it.
- Use current versions of Windows and *regularly update and patch*.
- Enforce strong password management policy with regular password changes.
- RDP access must be limited on an *"as needed" basis to those networks and accounts only*.
- Use of Virtual Private Network (VPN) with Multi-Factor Authentication (MFA) is *essential* when using RDP.

Remote Desktop Gateway (RDG)

What is RDG?

- Microsoft's "solution" to the numerous RDP-related security woes.
- RDG provides companies with capability to let employees remotely connect to the company's IT resources via any device with a Remote Desktop Client (RDC).
- Incorporates Multi-Factor Authentication (MFA) and encrypts RDP traffic using Transport Layer Security (TLS), a version of SSL (which is used to encrypt web browser traffic (i.e. https))
- As with RDP, RDG is easy to turn on and use. But *implementing RDG alone does NOT solve vulnerabilities* and risks associated to RDP.

Best Practices at using RDG

- *Patching and updates regularly. Only allow users via VPN* to gain access to RDG server.
- Multi-factor Authentication (MFA) *is essential on both* VPN and RDG.
- Network Segmentation is *essential*. (Think watertight deck hatches on ships)

Questions?

Alex Ricardo, CIPP/US
Breach Response Services

Beazley Group

Rockefeller Plaza
45 Rockefeller Plaza, 16th Floor
New York, NY 10111

t: +1 (212) 801 7111
c: +1 (646) 934 4100 – preferred
e: alex.ricardo@beazley.com

For More Information: www.beazley.com

"It's bad enough a company may possibly face liability from the data breach itself. The last thing you want is to create further liability exposure from how you respond to the incident.

Making sure you are kept in the best defensible position possible during the course of your breach response methodology should be a priority."