UNDERSTANDING THE CYBER THREAT LANDSCAPE

October 31, 2019
Our presenters

Bob Feldmann
National State & Local Government Industry Leader

Shan Grant
Security, Privacy & Risk Services Supervisor
KNOWING THE THREATS
A history of ransomware

- Has been around since 1989
  - AIDS Trojan or PC Cyborg
- Not all encrypt
  - Leakware or doxware
- The worst was WannaCry
  - 200k Computers in 150 countries
RANSOMWARE-as-a-Service

• Let’s talk about GandCrab
  - On the scene in Jan 2018
  - Off the scene mid 2019—complete shutdown
  - Reported as RaaS

All the good things come to an end.

For the year of working with us, people have earned more than $2 billion…
Earning with us per week $2,500,000.

We personally earned more than 150 million dollars per year. We successfully cashed this money and legalized it….
Yeah, it’s hard out here for a computer

- Tenets are the same
  - Patch your systems
  - Limit access to data and systems
    - Particularly write access

- Off-site/Offline backups or snapshot base backup service
- Good anti-virus/anti-malware
- Don’t trust anything
Ransomware recovery

- There’s no guarantee that all the data will be recovered.
  - Roughly 5–15% loss with a decryptor

- Business are down for an average of nine days.

- For complete recovery, it could take weeks to years. Consider:
  - System wipes
  - Recover from backups
  - Repeat the process for each server or computer
PERSONAL CYBER SECURITY
If you do it at home, you’ll do it at work

- Use a cloud-based password safe
  - Automatically generates a password
  - Prevents reuse of passwords
  - Checks for compromised passwords
  - Some allow document storage or personal detail storage
  - It’s in the cloud, but you can export it
- Use Multifactor Authentication (MFA)
  - Two or more of the below:
    - Something you know
    - Something you have
    - Something you are
- Consider a VPN provider
  - Research (google) them!
  - DNS Leakage
  - Working remotely—hop on corporate VPN

- Bitwarden
- 1password
- Dashlane
- Lastpass
- KeePassXC – not cloud based

https://www.wired.com/story/best-password-managers/

- Google Authenticator
- Authy
- Yubico

Why VPN and highly rated providers:
Other cool things about password managers

Great news! Not a single address you submitted has been compromised in a known security breach since the last time you ran this test. Next you'll get your score and some tips for improving your security.

Step 1 - Change Compromised Passwords
Step 2 - Change Weak Passwords
Step 3 - Change Reused Passwords
Step 4 - Change Old Passwords
You are your own company

• Segregation of duties—(SOD)
  • SOD is a basic building block of sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Without this separation in key processes, fraud and error risks are far less manageable. (source: AICPA)

• Identity Theft Monitoring
  • Also Identity Theft Insurance or, more generally, Personal Cyber Insurance
  • Legal fees, loss access to credit, late fees and other costs
  • Anxiety every time you check the mail

• DIY
  • Review your financial statements
  • Configure alerts for charges, balance transfers, payments
    • Take advantage of thresholds for the notifications so they don’t become annoying
  • See all your financial details at a glance using Personal Capital, Mint, or Quicken (dying a slow death)
    • These services do aggregated research with your data so read the fine print
GIMME SOME MO’ PRIVACY
Going down privacy lane

- 1945: Rise of Information Technology
- Fair Credit Reporting Act of 1970
- Privacy Act of 1974
- 1980: Freedom of Information Act
- OECD Guidelines and International Privacy
- Cable Communications Policy Act of 1984
- Electronic Communications Privacy Act of 1986
- Health Insurance Portability & Accountability Act of 1996
- Children’s Online Privacy Protection Act of 1998
- Gramm-Leach-Bliley Act of 1999/2001
- Data Protection Directive
- General Data Protection Regulation
- 2018/2020: Consumer Protection Act
- ?
**How is CCPA different than GDPR?**

**Different consumer rights:**

<table>
<thead>
<tr>
<th>Rights Covered</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to know and of access</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Right to deletion/erasure</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Right to restriction of processing</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Right to data portability</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Right to object</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Right to opt of out sale</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Right to equal service and price</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Right to opt In (minors under 16)</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

In addition to compliance, it’s really all about the data—what type of data and how it is used.

Data governance and management programs should consider mapping for both.
Privacy Cliff Notes

- Nevada Online Privacy Law
- New York Privacy Act
- Maine Act to Protect of Online Consumer Information
- Massachusetts Data Privacy Law
- Hawaii Consumer Privacy Protection Act
- Maryland Online Consumer Protection Act
BE VIGILANT
BE AWARE
Some personal security suggestions

**Security, security**
- Always ask why someone needs your information
- Do not use public Wi-Fi
- People actually “dumpster dive”

**Social engineering**
- “Delivery person,” “corporate IT”
- A LinkedIn “recruiter” or “met you at a conference” request to add you to their network

**Too much information (TMI)**
- Geolocation tagging in photos or social media posts
- Be careful what you post on social media
Questions?

Shan Grant
Supervisor
Security, Privacy & Risk Services

Shan.Grant@rsmus.com
https://www.linkedin.com/in/shan-grant/

- 15+ years security and privacy experience
- Originally from Brooklyn, New York; moved to Florida 2018
- PCI QSA and PA-QSA, CISSP, CISA, Fair Credit Reporting Act (FCRA) Certification
- Worked and designed compliance programs for financial entities, fintechs, healthcare/healthtech, and non-profit
- Specializing in regulated environments:
  - Payment Card Industry (PCI)
  - HIPAA
  - CRA (FCRA)
  - FDIC/FFIEC
  - Data Privacy
- Career Highlight: Worked Cannes Film Festival
THANK YOU FOR YOUR TIME AND ATTENTION