Cybersecurity Trends & Lessons Learned in 2020

October 7, 2020

Presenters: Rob Wilkinson, David Menichello

Agenda

- Pulse on InfoSec
  - Business Trends
  - Attackers
- Information Security Fundamentals
- Ransomware Case Study (Blackbaud)
- Work from Home Case Study
- Review and Recap
- Questions and Answers

Pulse on Information Security and Risk Trends

Pulse – Business & Technology

Shift to the Cloud
e.g. AWS, Office 365, SaaS Applications, Monthly Subscription Fees

Increased outsourcing
Requires personnel & process to assess and monitor **vendor *risk***

Increased data sprawl (mobile, cloud services, low storage costs)
Companies challenged with tracking, controlling and securing data

More demanding data privacy regulations
CCPA, GDPR, NYDFS, HIPAA, GLBA, COPPA…
Stringent requirements and significant penalties for non-conformance

Pulse – The Attack Side in 2020

Attackers are: Financially Motivated & Organized

- Cybercrime an **$8b industry & climbing**
- 86% of attacks financially motivated
- 70% of breaches were External Actors
- 55% of attackers are part of organized crime groups
- Only 4% of data breaches required > 4 attacker actions

Attackers are: Agile, Sophisticated, and Automating

- Organized groups have monthly quotas for compromising data
- Phishing attacks increasing and becoming more sophisticated - 45% breaches involved hands-on "hacking."
- 37% attacks utilized credentials stolen from other websites (credential 'stuffing' instead of credential 'cracking')

Attackers are: not Discriminating

- 58% of victims had personal data compromised
- 28% of breaches involved small business victims, 72% large business
- Most small and mid sized companies are simply outgunned

https://enterprise.verizon.com/resources/reports/dbir/

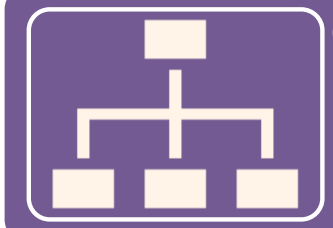
Pulse – The Non-Profits' Challenges

Striking a Balance

- Functional security requires balance between people, process and technology
- Outsource / Insource, Short Term / Long Term, Buy / Build
- Culture of continual improvement and addressing **root causes**

The Tools Trap

- Significant over-reliance on tools to fix security issues
- Tendency to continue to bolt-on vs. **bake-in**
- Metrics are confusing, incomplete and lack transparency



Organizational Challenges

- IT tries to do security in their spare time
- Lack of IT Governance can put companies pursuing change at increased risk
- Security fails to put issues into the **business context,** often lacking representation in leadership meetings

Fundamentals

Patch Software without Delay

Use Strong Passwords with Multi Factor Auth.
Different Passwords Across all Applications

Limit Access to Data
Especially at Home

Improve Threat Monitoring ($)
(the breach should not be the alert)

Culture of Awareness
(**Phishing**, Social Engineering, Stigma)

63%

of confirmed data breaches involved **weak, default or stolen** passwords

Case Study: Blackbaud

Case Study – Blackbaud

What Happened?

- *Blackbaud was the victim of a ransomware attack in May 2020*
- *The cybercriminal was able to steal a copy of Blackbaud backup files, which included at least 6 million customer records*
- *Affected schools, faith communities, foundations, healthcare organizations, nonprofit organizations…*

Data Breach

- Attacker was inside the network, found & exfiltrated data undetected
- Ransomware was triggered *after* data was stolen
- BB kept the event under wraps from May to July

12	Matt Ondesh	8/14/76	138-23-3264	132 Maritime Lane	Atlantic City	NJ	08401	609-425-0875
13	David J. Wicet	1/5/56	636-42-0925	9000 Dee Ln. Apt. 3	Egg Harbor Twp	NJ	08234	609-371-4254
14	Sandra Dunkin	3/18/80	291-54-9283	724 Packer Ln	Green Bay	WI	75321	703-835-2512

Ransomware

- BB was threatened: "pay the ransom or we will publicize the stolen records."
- **Paid the Ransom** and received *'certificate of destruction'*
- Recover operations, notify customers, lawsuits, reputational damage, **lasting impact**.

Lessons Learned

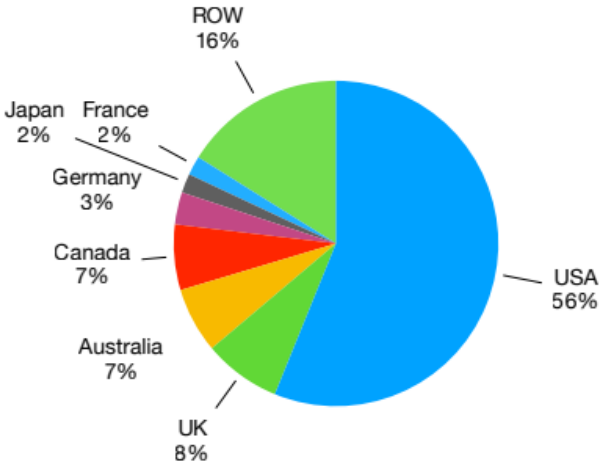
- IDENTIFY: Know where sensitive data is stored
- PROTECT: Have a backup & keep data isolated
- DETECT: Monitor network for anomalies
- RESPOND: Prepare IT and Legal to react swiftly
- RECOVER: Plan customer communications

Blackbaud is not Unique

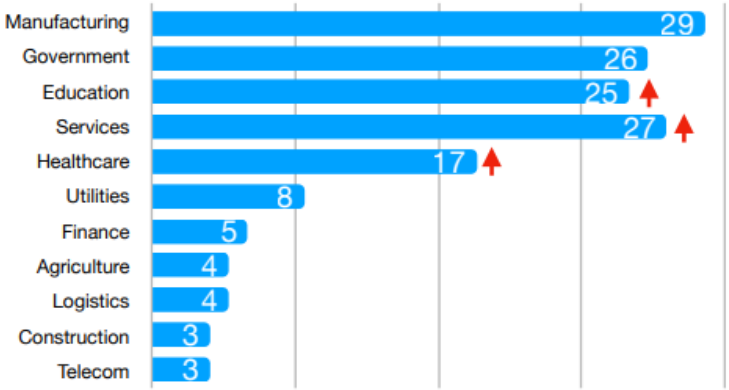
Global Ransomware Report - January to September 2020

blackfog.com

Attacks by Country



Attacks by Industry



Key Trends

Average ransomware payment

US$178,254 +60%

62% of all attacks Ransomware

80% of attacks exfiltrate data

Case Study: Remote Worker

Information Security Essentials – Home Workers

Most likely Threats: Device Loss/Theft, Malware, Hacking

Best Practices

- **only use company-approved devices** (anti-virus, patching)
- **limit use of personal devices** and browsers (comingling passwords)
- enable encryption both **at-rest** and **in-transit**
- store data assets (laptop, paper files) in centralized, safe place.
- on public Wi-Fi, use VPN to proxy internet traffic through office.
- continue to be wary of phishing emails, now pandemic-themed.

Phishing: What to Look For

- Similar but incorrect domain name
- Alarming content
- Attractive offers
- Push for immediate action
- Spoofed sender
- Legitimate looking content
- Incorrect grammar
- Fraudulent links

Q&A

Thank you!

rob.wilkinson@btbsecurity.com

david.menichello@btbsecurity.com