CYBER HOSPITALITY

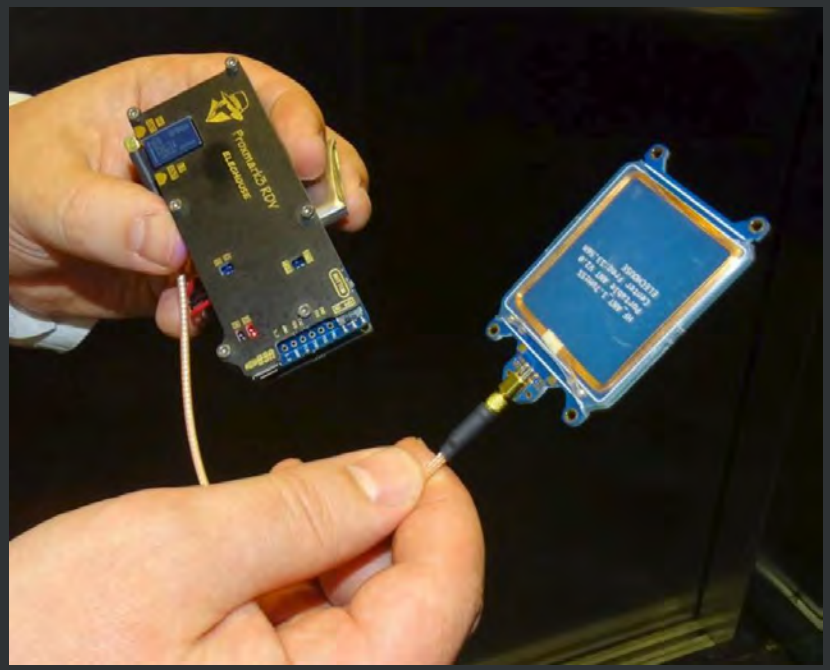
David Caswell, PhD
US Air Force Academy


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Cyber

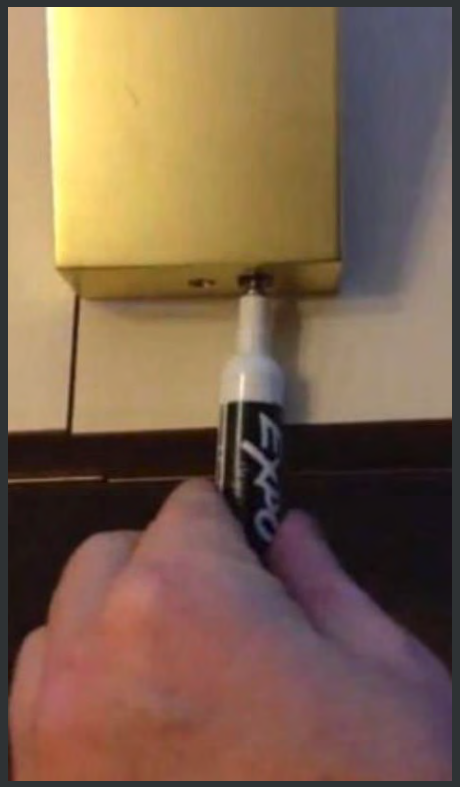
- "of, relating to, or involving computers or computer networks (such as the Internet)" – Merriam Webster

Electronic Key Systems

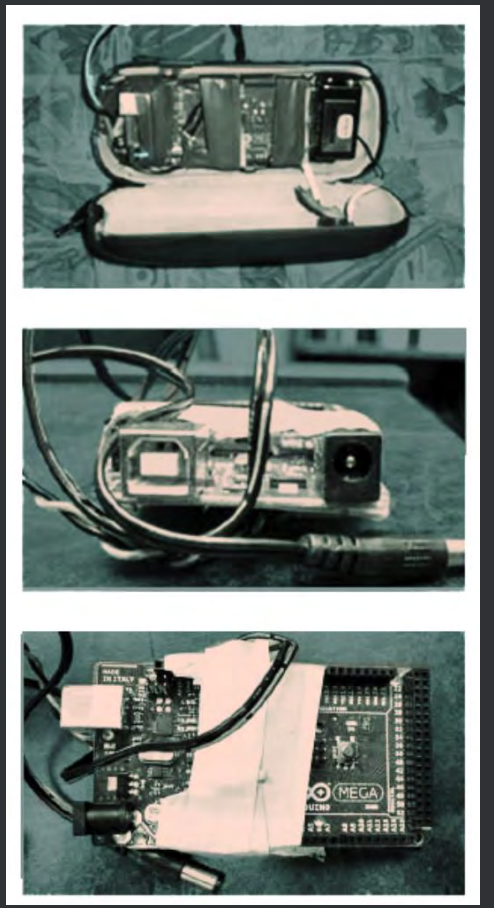


Master key for Assa Abloy locks (2018)

- Patched with Feb 2018 Update



Onity door locks (2012)



Hotel Cyber Incidents

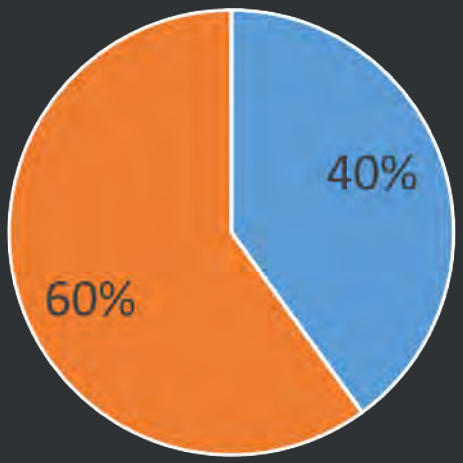
- 2018 – Huaza Hotels Group, Ltd
  - 130 million hotel chain guests records
- 2017 - Sabre Hospitality Solutions' SynXis hotel-reservations system
  - Four Seasons, Trump Hotels, Hard Rock Hotels & Casinos, and Loews Hotels
  - Payment data over 7+ months
- 2015 – Hilton Worldwide, Hyatt, Mandarin, Starwood Hotels and Resorts
  - Payment data for 250 hotels
- 2008 – Wyndham
  - 3 independent hacks on guest records
  - 619,000 accounts stolen
  - $10.6M of fraud loss

Cyber Security: Hospitality Industry

"Hotel chains are often behind the cybersecurity curve, making them more vulnerable to attacks."

- Shlomo Touboul, CEO of Tel Aviv-based Illustive Networks (stylized illusive networks)

- Corporate/internal network breach
- Property Management



- Electronic Key Systems
- Wi-Fi networks
- Data sharing networks with third parties
- Point of Sale (POS)

Trustwave 2018 Global Security Report

World's Biggest Data Breaches

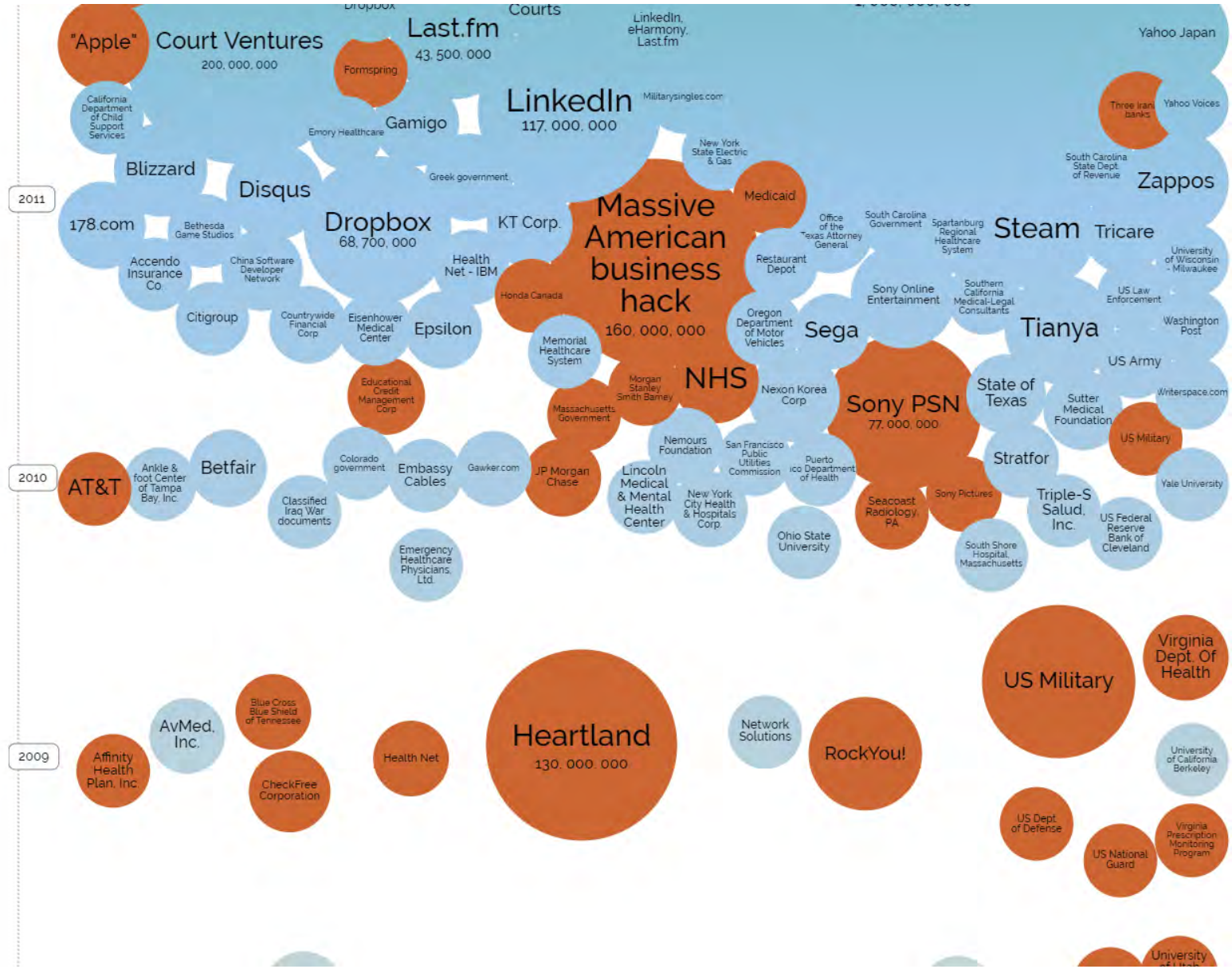
Selected losses greater than 30,000 records

(updated 15th Oct 2018)

interesting story

YEAR

BUBBLE COLOUR | YEAR | METHOD OF LEAK | BUBBLE SIZE | NO OF RECORDS STOLEN | DATA SENSITIVITY | HIDE FILTER



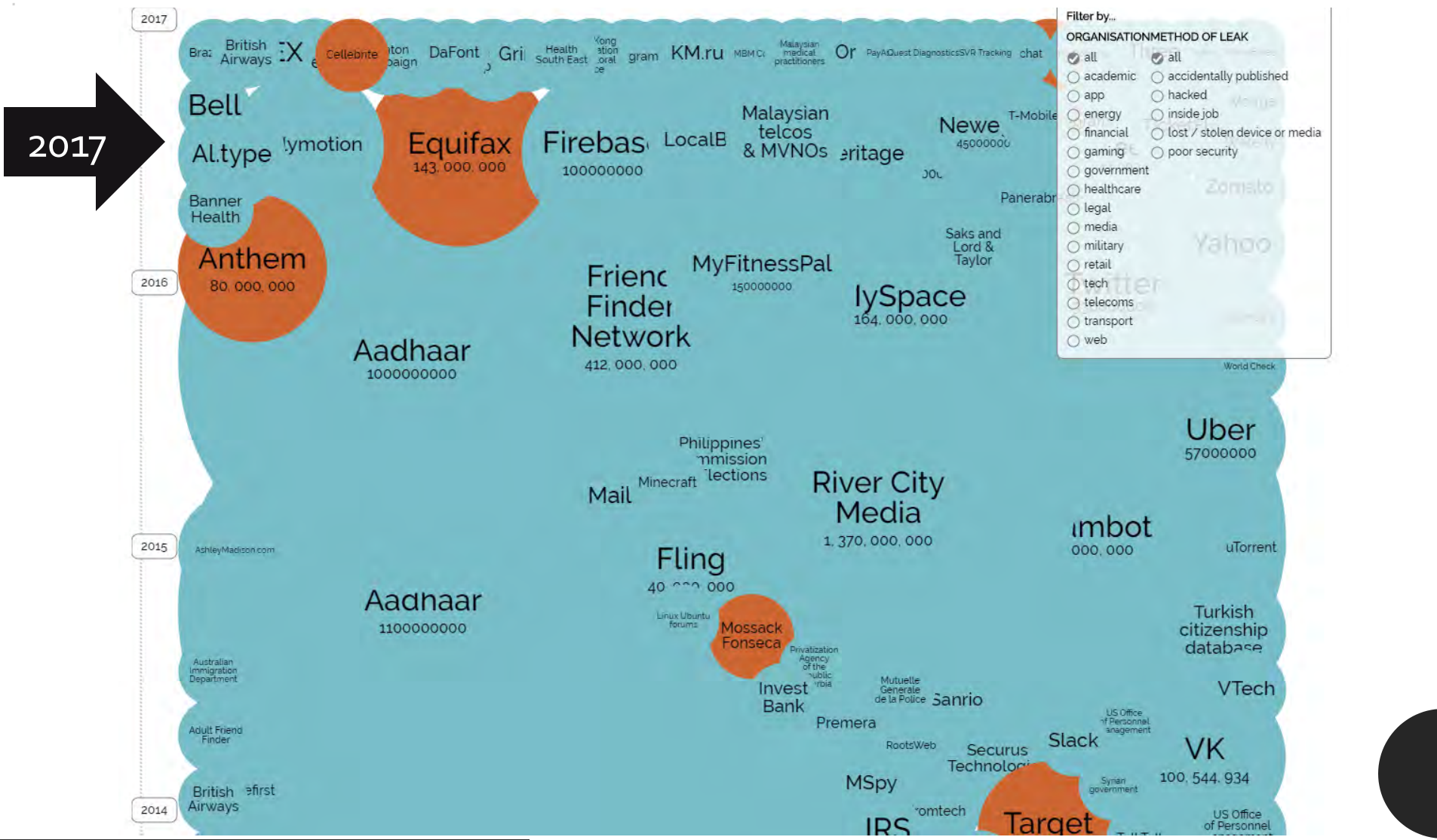
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 15th Oct 2018)

interesting story

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | HIDE FILTER



DATA COMPROMISE

Industries most affected

17% Retail

13% Finance & Insurance

12% Hospitality

40%

of breaches targeted payment card data

22% Magnetic stripe

18% Card-not-present

Incidents involving point-of-sale systems were most common in North America, which has been slow to adopt the Europay, MasterCard and Visa (EMV) chip standard for payment cards

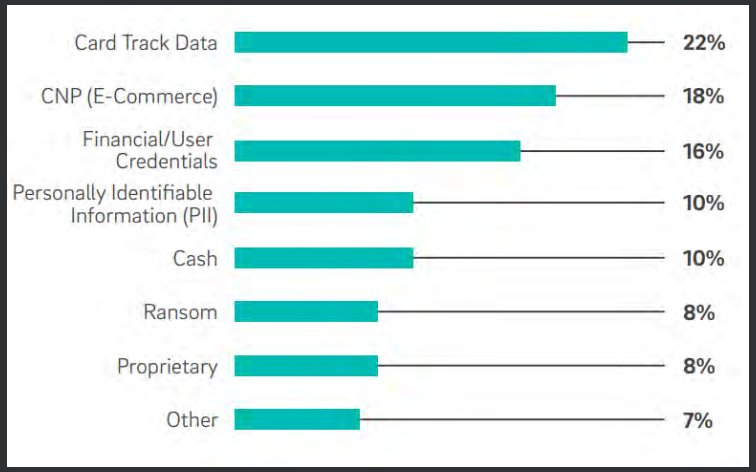
Median number of days between intrusion and detection for detected incidents

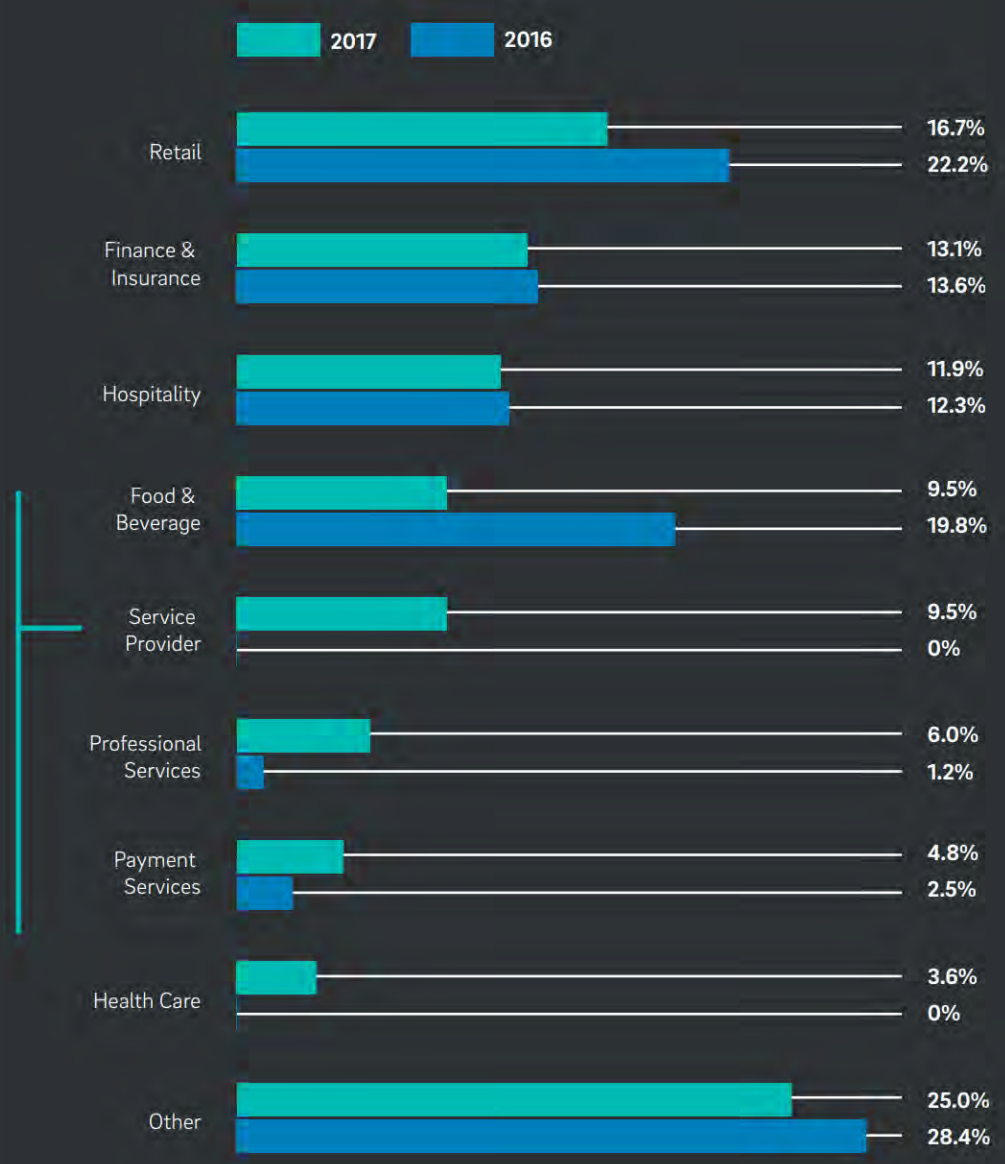
0 INTERNAL

83 EXTERNAL

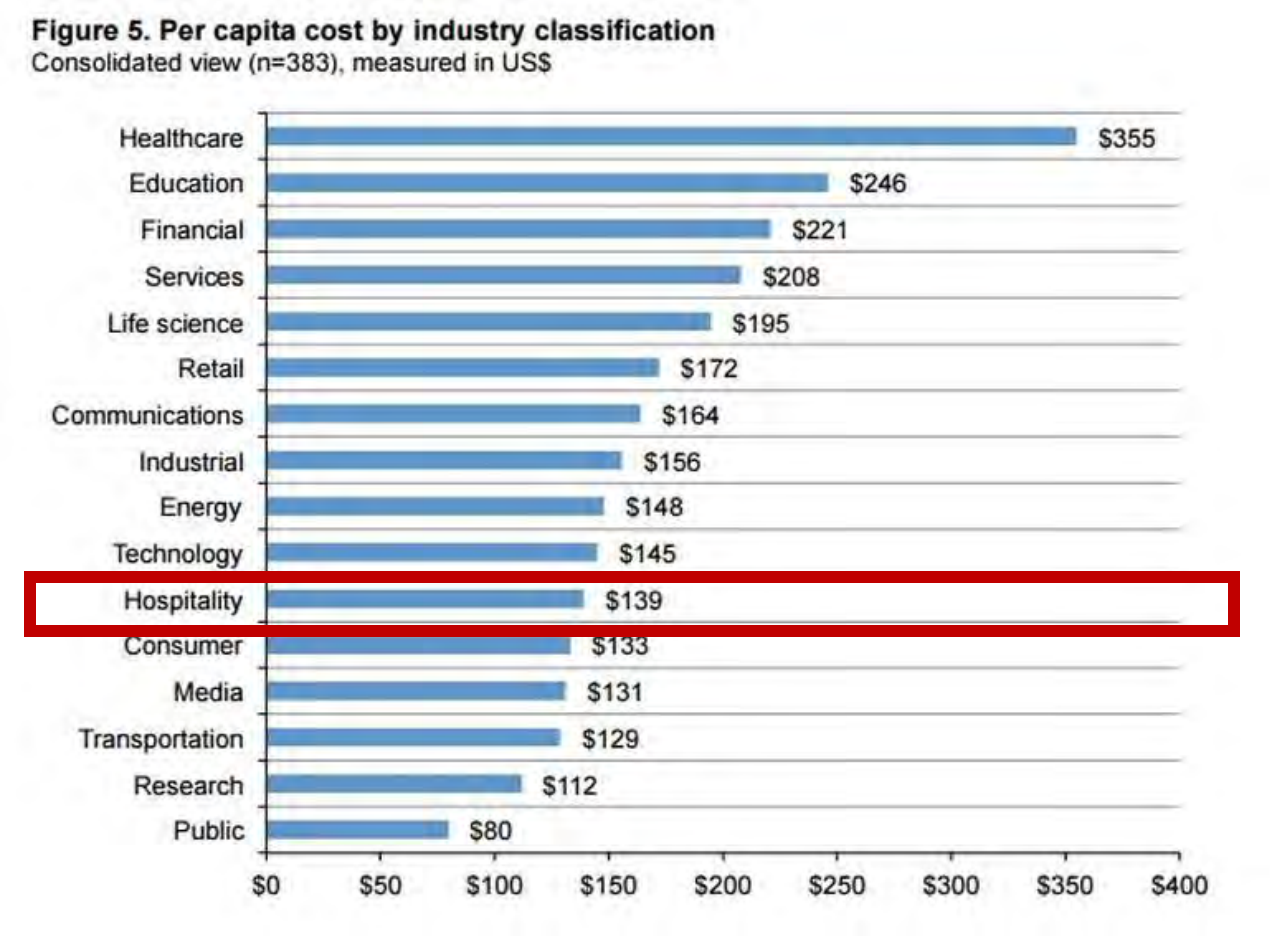
Trustwave 2018 Global Security Report

Data Compromise by Industry





Per Capita Cost of Data Breach



Ponemon Institute, 2018, https://www.ibm.com/security/data-breach

Top Methods of Compromise

POS

- **47%** Phishing/Social Engineering
- **23%** Remote Access
- **13%** Malicious Insider
- **7%** Weak Password
- **7%** Other
- **3%** Misconfiguration

Corporate/ Internal Network

- **55%** Phishing/Social Engineering
- **13%** Malicious Insider
- **9%** Remote Access
- **8%** Misconfiguration
- **7%** Other
- **5%** Code Injection
- **3%** Weak Password

E-Commerce

- **45%** File Upload
- **39%** Code Injection
- **13%** Remote Access
- **3%** Weak Password

Trustwave 2018 Global Security Report

Phishing & Social Engineering

- Emails from "management" on policies (with pdfs containing malware)
- Photos of complaint evidence (with embedded malware)
- "Please can I use the computer, I lost my passport and phone…"
- "I locked my key in my room"

Ransomware

- $133,000: average amount lost in recovery costs following ransomware incident

-Sophos "The State of Endpoint Security Today," 2018

Information Technology Attacks

Hospitality

78% Card Track Data
11% PII
11% Ransom

Food & Beverage

70% Card Track Data
20% Ransom
10% E-Commerce

Trustwave 2018 Global Security Report

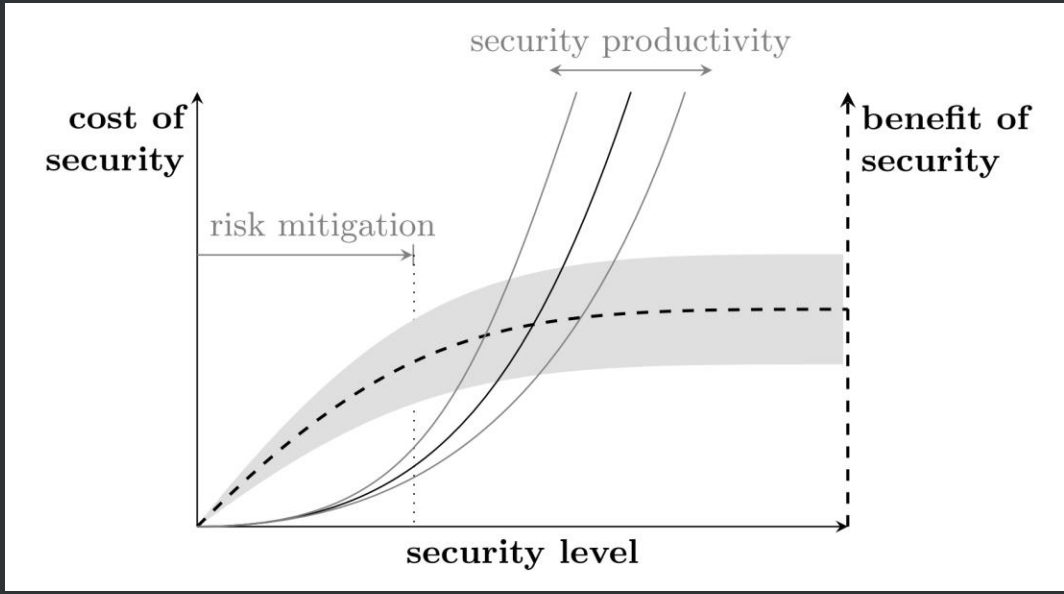
Liability

"The FTC did not 'allege that Wyndham used *weak* firewalls, IP address restrictions, [or] encryption software. Rather, it allege[d] that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, [and] did not use *any* encryption for certain customer files.' Furthermore, the company was not hacked just once, but three times, and the second and third hacks occurred after Wyndham had knowledge of the first breach."

Harvard Law Review, FTC vs Wyndham Worldwide

Risk-Cost Tradeoffs

- Ability to function without the system?
- Cost to rebuild/redeploy the system?
- Impact to your business if customer data is stolen?
  - Customer trust is lost?



Bohme, Rainer, Security Metrics and Security Investment Models, 2010

Mitigations: Technology

- Leverage best practice network design
  - Strong Next-Gen Firewall (NGFW)
  - Web application firewalls
  - Intel based Intrusion Protection Service
- Ensure security devices are well-configured
- Patch everything often!
- Segment customer internet from business services
- Strong passwords for accessible business systems
- Backup your systems

Mitigations: People

- Train for a defensive mindset
- Business Continuity
  - Run a disaster exercise
  - Test backup/restoral plan

AF Cyber Innovation Center

Bringing the Future Faster

AIR FORCE CYBERWORX™

References

- Toubol, Shlomo, How Travelers Can Stay Safe From Cyberattacks Over the Holidays, 2016, http://fortune.com/2016/12/20/cybersecurity-holiday-travel-vacation-hotels/
- http://mcgowanprograms.com/blog/4-reasons-hotels-need-cyber-insurance/
- https://www.hotelmanagement.net/tech/cyber-insurance-indispensible-to-hospitality-risk-management
- https://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/
- https://www2.trustwave.com/GlobalSecurityReport.html
- https://www.wired.com/2017/08/the-hotel-hacker/
- https://informationsecurity.uibk.ac.at/pdfs/Boehme2010_SecurityInvestment-IWSEC.pdf

Topics

- Everyone, including all businesses, must be prepared for a wide range of increasing and sophisticated cyber threats. Cyber-readiness is no longer just a government or IT department responsibility. The implications of global cyber risks to national, regional, and local infrastructure (electricity, water, emergency services), and other services such as banking, credit card processing, and digital communications require that every hotel have its own Cyber Readiness plan and team.

- Attendees will learn:
  - The U.S. Airforce Academy Center of Innovation (COI) and WHY its focus on Cyber
  - Cyber has expanded beyond hacking. How does this impact the commercial marketplace?
  - The evolution of Data Security? How data manipulates? How is data (customers' data) protected? What are the Cyber considerations between Data Storage vs Operations?
  - What is the broader definition of Cyber?
  - How is the DOD partnering with Commercial Industry?