BAIRD HOLM LLP
ATTORNEYS AT LAW
EST. 1873

© 2016 Baird Holm LLP

CYBER THREAT 2021: Your Employees are Still Your Weakest Link

Robert L. Kardell

Attorney, Ret. FBI, MBA, CPA, CISSP, CFE, CFF, GSEC, A+, Net+,

BKardell@BairdHolm.com

Part I – Costs of Cyber Attacks

© 2019 BAIRD HOLM LLP

Costs of Breach

- IBM Ponemon Study - 2019
  - $250 Avg. (US)
  - $429 Healthcare Avg.

© 2019 BAIRD HOLM LLP

Costs of Breach

- Cyentia

Records	Probability of At Least This Much Loss					
	$10K	$100K	$1M	$10M	$100M	$1B
100	82.0%	49.9%	17.8%	3.3%	0.3%	0.0%
1K	88.4%	60.9%	26.0%	5.9%	0.7%	0.0%
10K	93.0%	71.1%	35.8%	10.0%	1.4%	0.1%
100K	96.0%	79.8%	46.7%	15.8%	2.7%	0.2%
1M	97.9%	86.7%	57.7%	23.5%	5.0%	0.5%

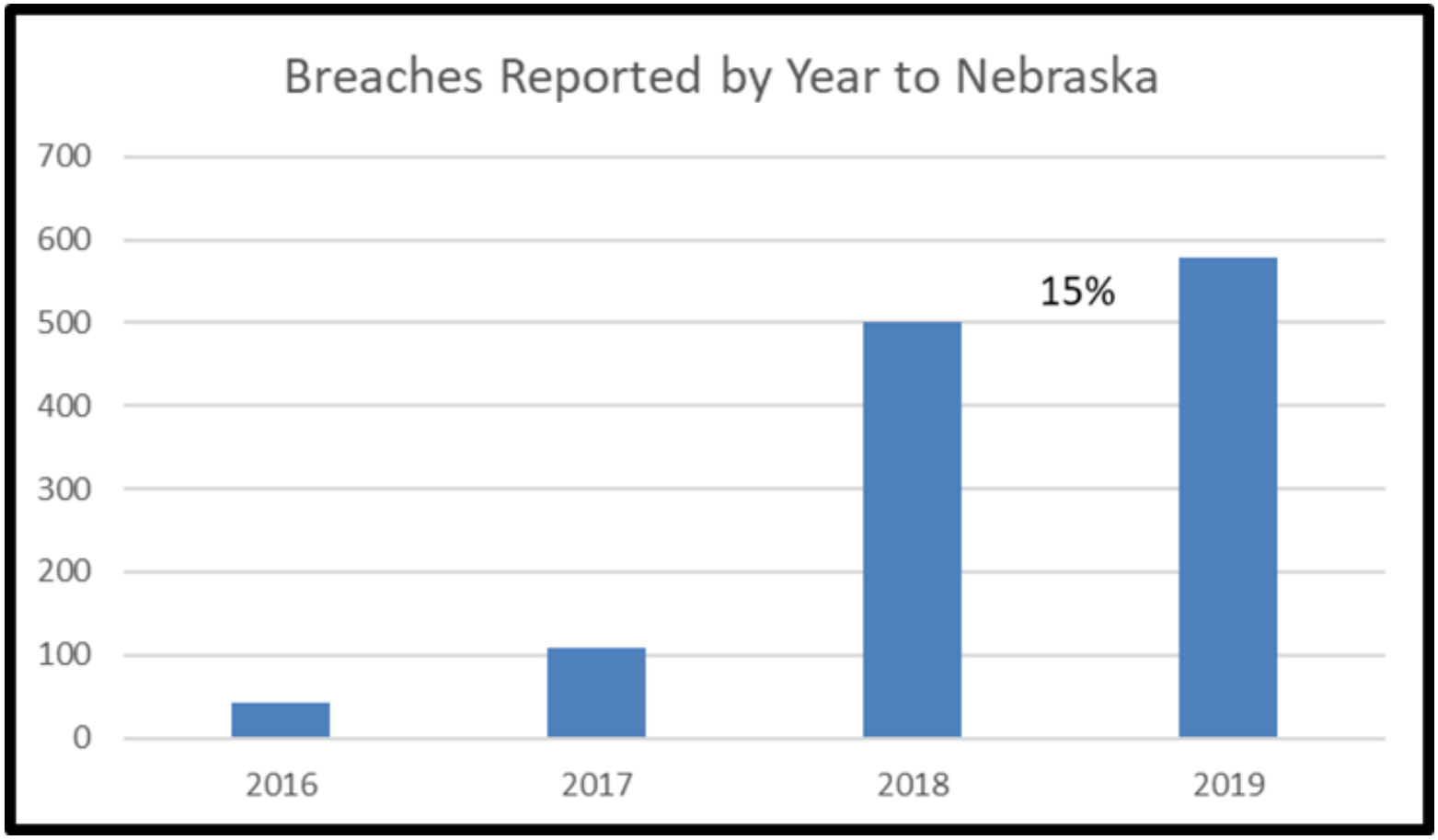
© 2019 BAIRD HOLM LLP

Nebraska Breach Statistics

Data Description	Total Records	Nebraska Records
Cost per Record (IBM Report)	$ 250.00	$ 250.00
Total Number of Breach Reports	1231	1231
Total Number of Records	5,730,377,134	2,376,143
Total Estimated Cost	$ 1,432,594,283,500.00	$ 2,925,032,033.00
Average Records per Report	4,655,059	1,930
Total Average cost per incident	$ 1,163,764,649.47	$ 482,563.57
2019 Breaches Only	578	578
Victims	118,321,349	326,933
Average Victims	204,708	566
Total Average Response Cost	$ 51,177,054.07	$ 141,407.01
2019 for Nebraska Companies	34	34
Victims	106,767	58,631
Average Victims	3,140	1,724
Total Average Response Cost	$ 785,051.47	$ 431,110.29

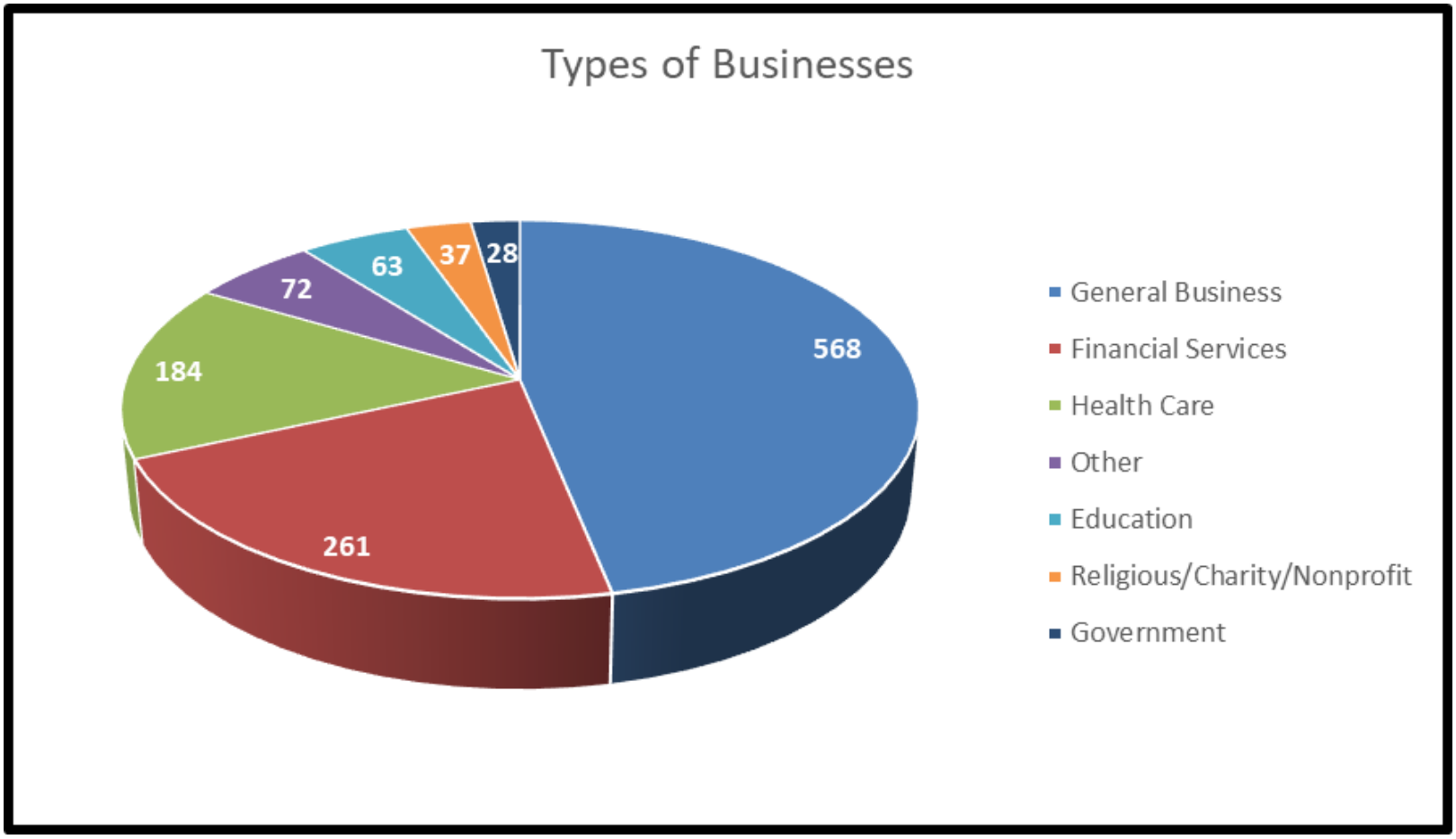
© 2019 BAIRD HOLM LLP

Nebraska Breach Statistics



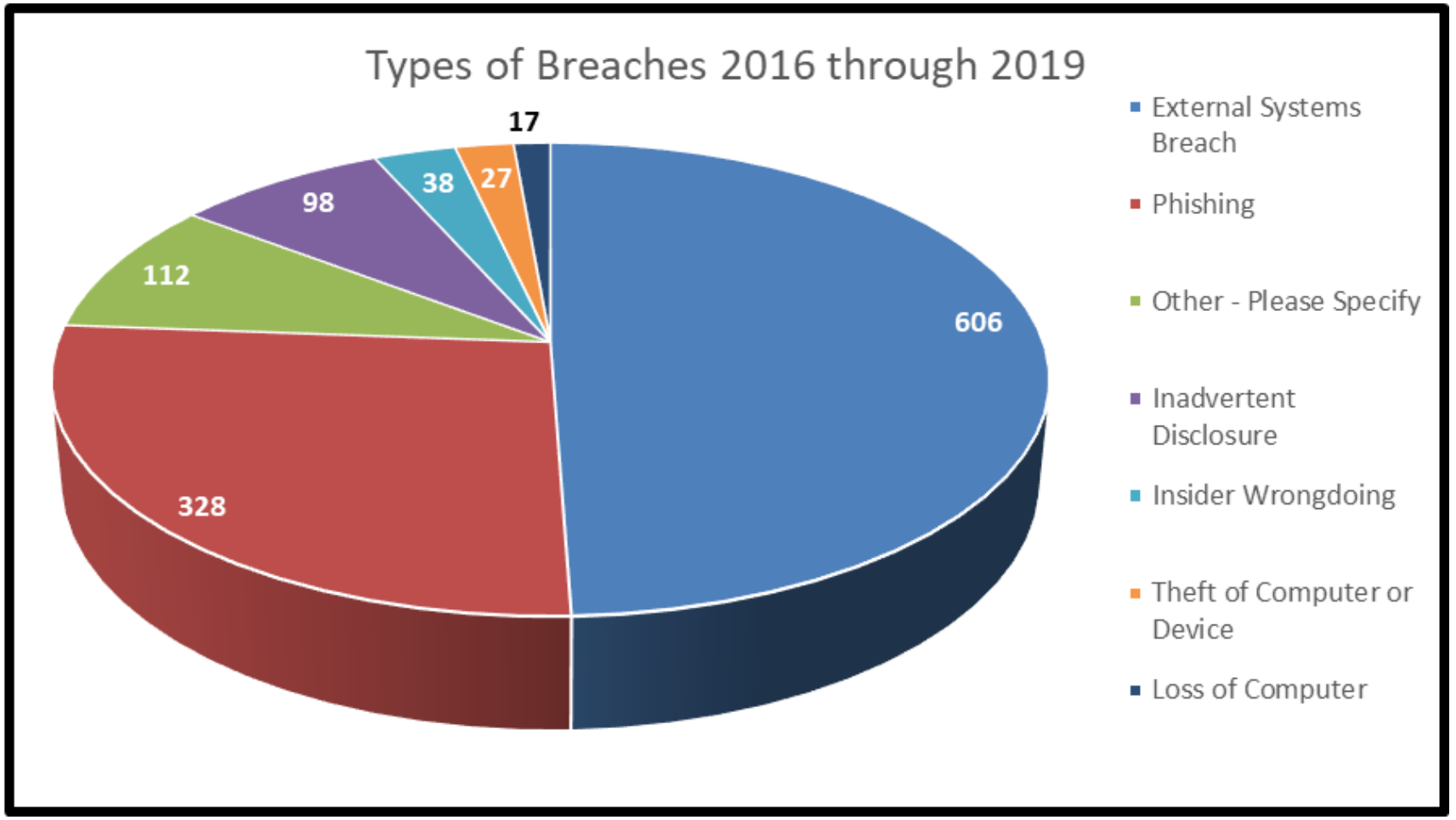
© 2019 BAIRD HOLM LLP

Nebraska Breach Statistics



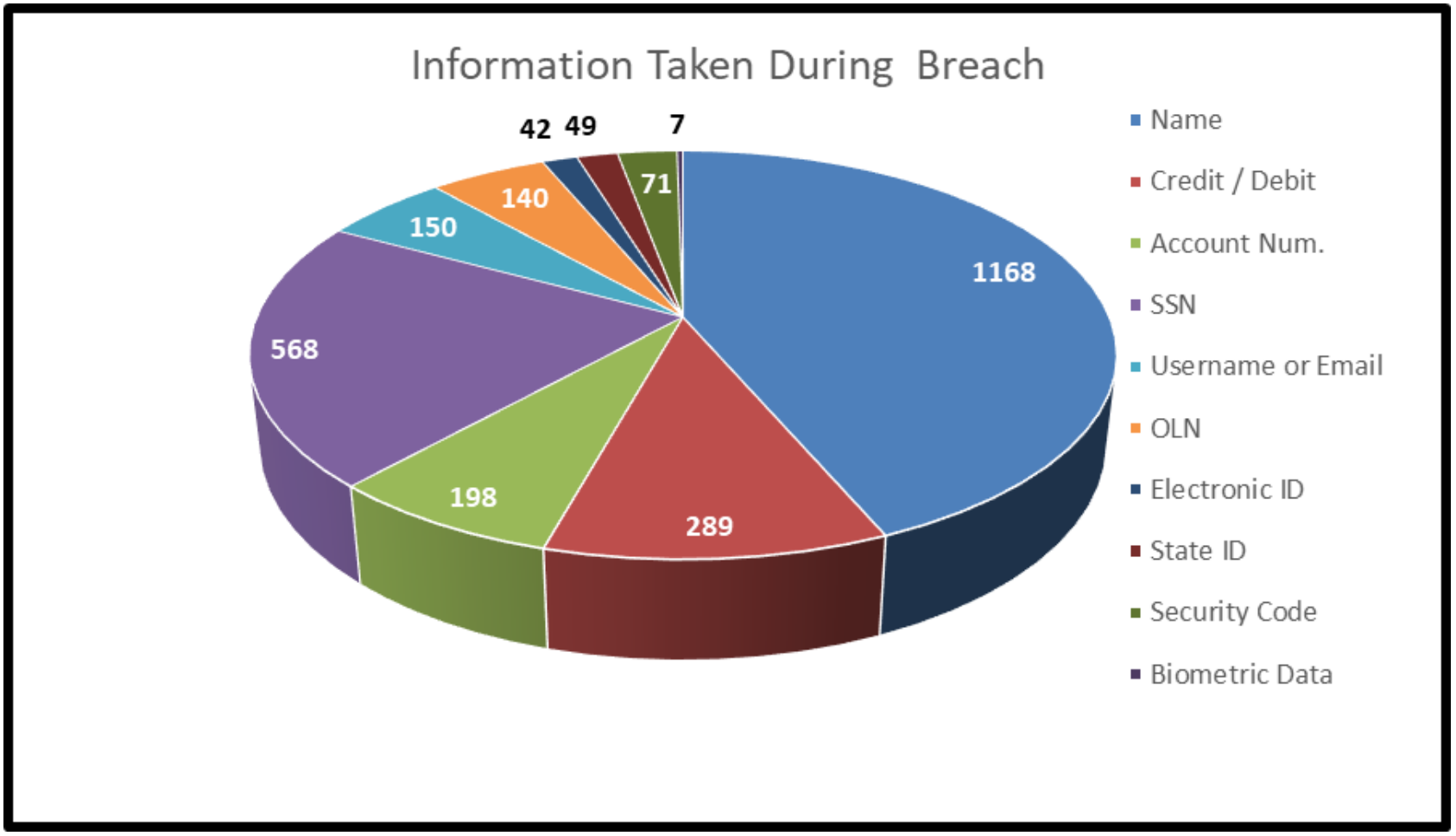
© 2019 BAIRD HOLM LLP

Nebraska Breach Statistics

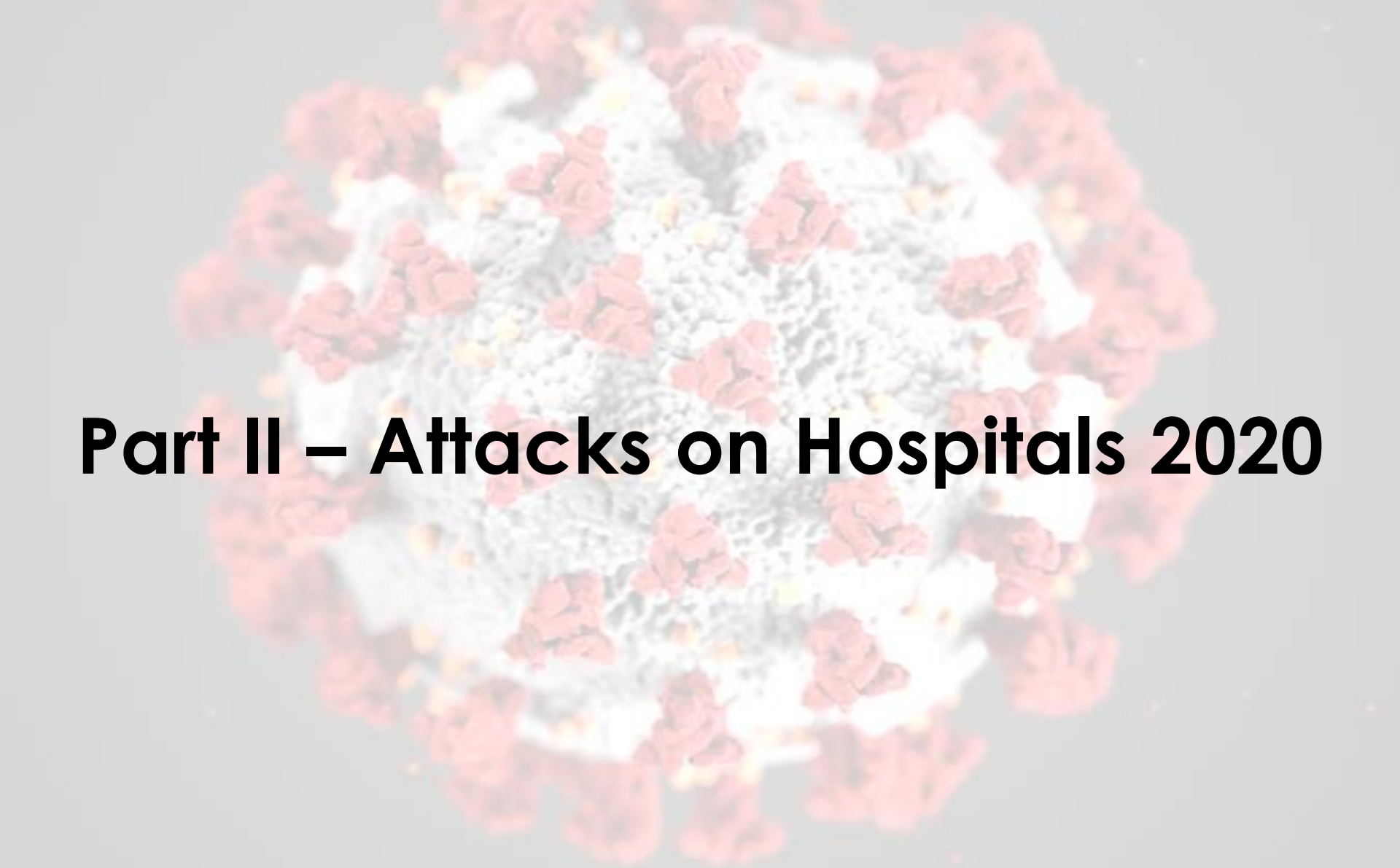


© 2019 BAIRD HOLM LLP

Nebraska Breach Statistics



© 2019 BAIRD HOLM LLP



Part II – Attacks on Hospitals 2020

© 2019 BAIRD HOLM LLP

Headlines

Healthcare providers that underwent cyberattacks in 2020 so far

Original release date: October 28, 2020 | Last revised: November 02, 2020

Print Tweet Send Share

Summary

This advisory was updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.

© 2019 BAIRD HOLM LLP

Ransomware Attacks

- Up 148% in March 2020 alone
- Study shows that cost of recovery doubles with ransomware

© 2019 BAIRD HOLM LLP

Exfiltration of Data

- Cyberattacks involving both data exfiltration and ransomware have increased 152% between Q1 and Q2 2020

© 2019 BAIRD HOLM LLP

Anatomy of an Attack

- Entry to network
- Movement of tools to network
- Reconnaissance of network
- Retreat to code
- Re-entry to network and
  - Deploy
  - Deploy and destroy
  - Remove, deploy, and destroy

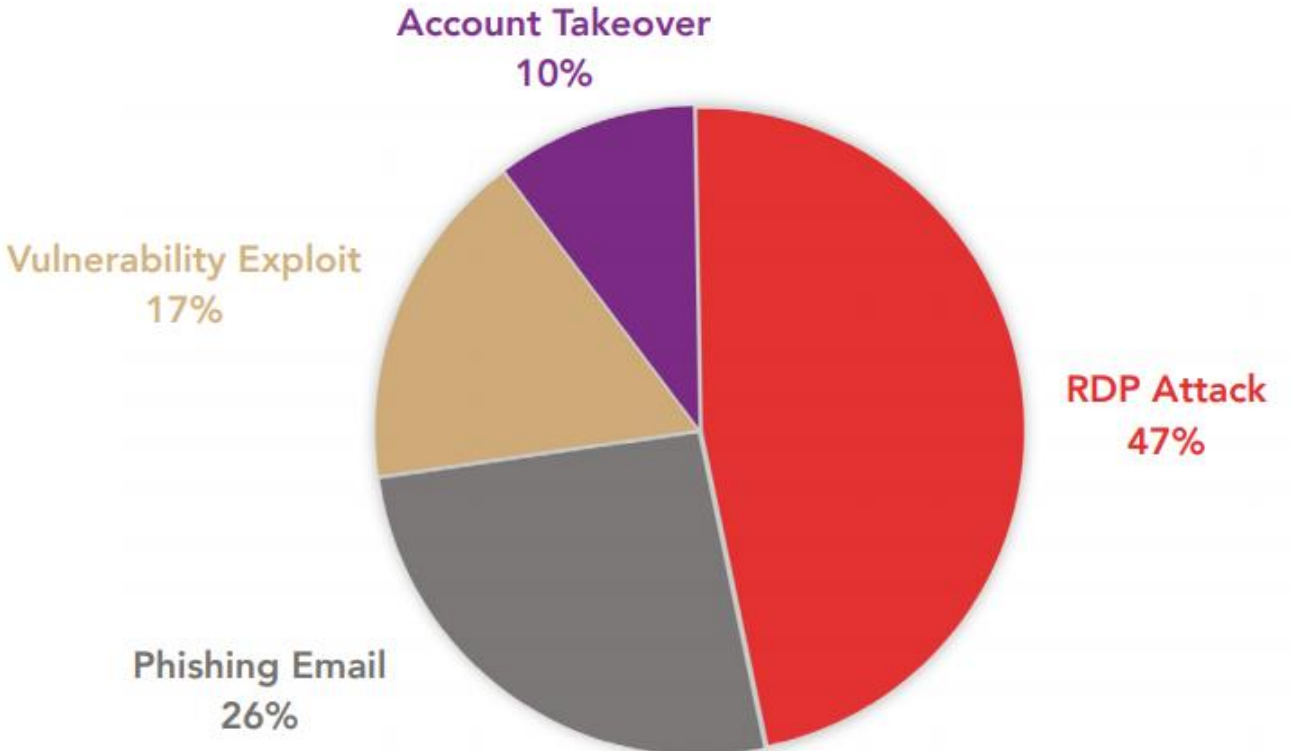
© 2019 BAIRD HOLM LLP

Entry to Network: Mitre Attack Vectors

1. Drive-by Compromise
2. Exploit Public-facing Application
3. **External Remote Services**
4. Hardware Additions
5. **Phishing**
6. Removeable Media
7. Supply Chain
8. Trusted Relationships
9. **Valid Accounts**

© 2019 BAIRD HOLM LLP

Attacks



© 2019 BAIRD HOLM LLP

Variants of Ransomware

- Gain Entry:
  - TrickBot
  - BazarLoader/BazarBackdoor
  - Emotet
- Encryption deployment
  - Ryuk
  - Conti
  - REvil

© 2019 BAIRD HOLM LLP

Remote Desktop Protocol

- More people working from home
- "RDP brute-force attacks grew by 400% in March and April"
- Defense:
  - Passwords
  - Strong Passwords
  - MFA
  - Update Software

© 2019 BAIRD HOLM LLP

Phishing

- More people working outside of controlled or monitored environment
- Defense:
  - Training!!
  - MFA
  - Monitoring of emails \ Spam protection
  - Domain protection

© 2019 BAIRD HOLM LLP

Valid Accounts

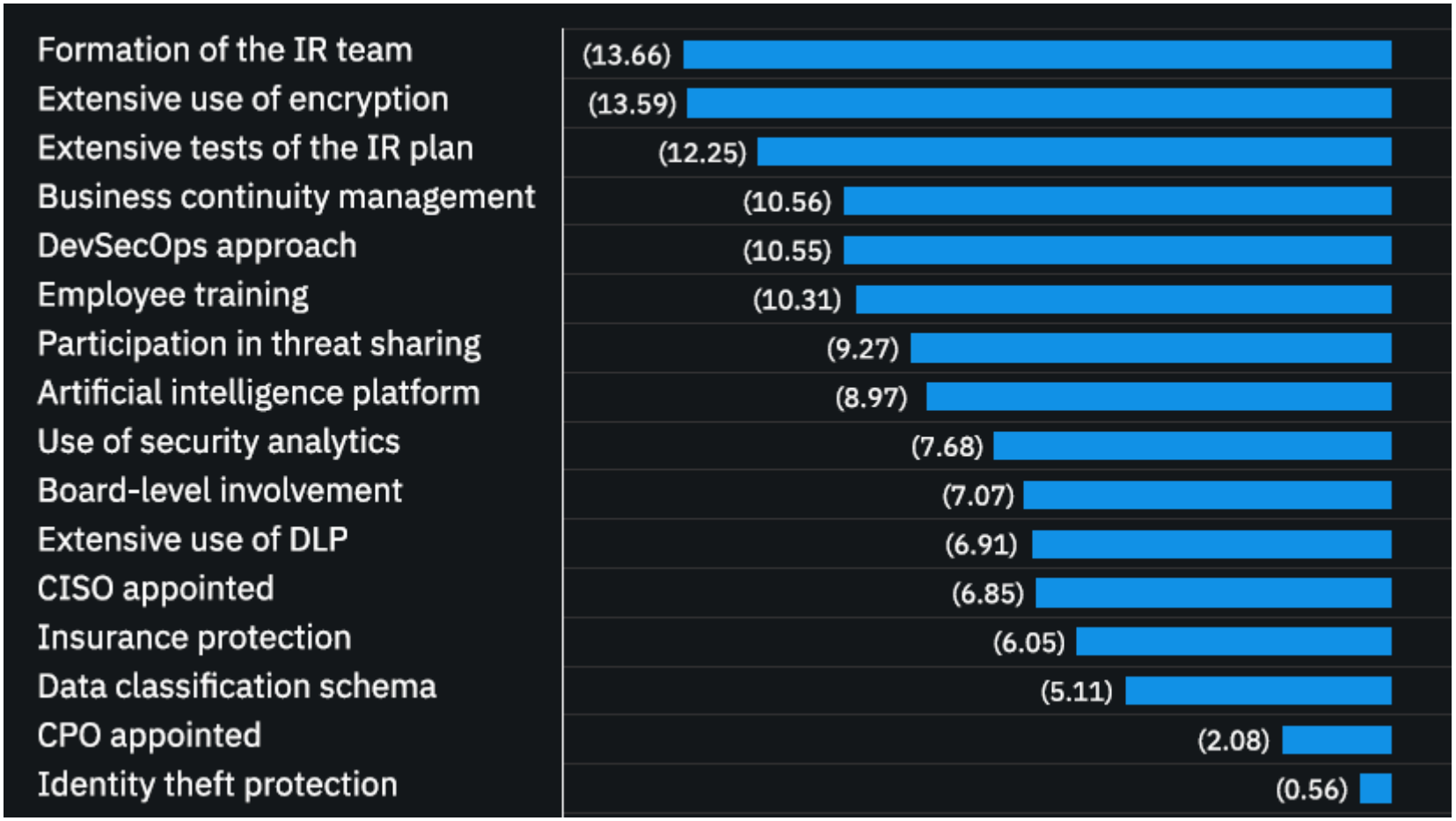
- 30 Billion usernames and passwords on Dark Web
- Defense:
  - Do not reuse passwords
  - Use harder passwords for more sensitive sites
  - Check for compromised passwords
    - Haveibeenpwned.com

© 2019 BAIRD HOLM LLP

Part III – Cyber Defense Value

© 2019 BAIRD HOLM LLP

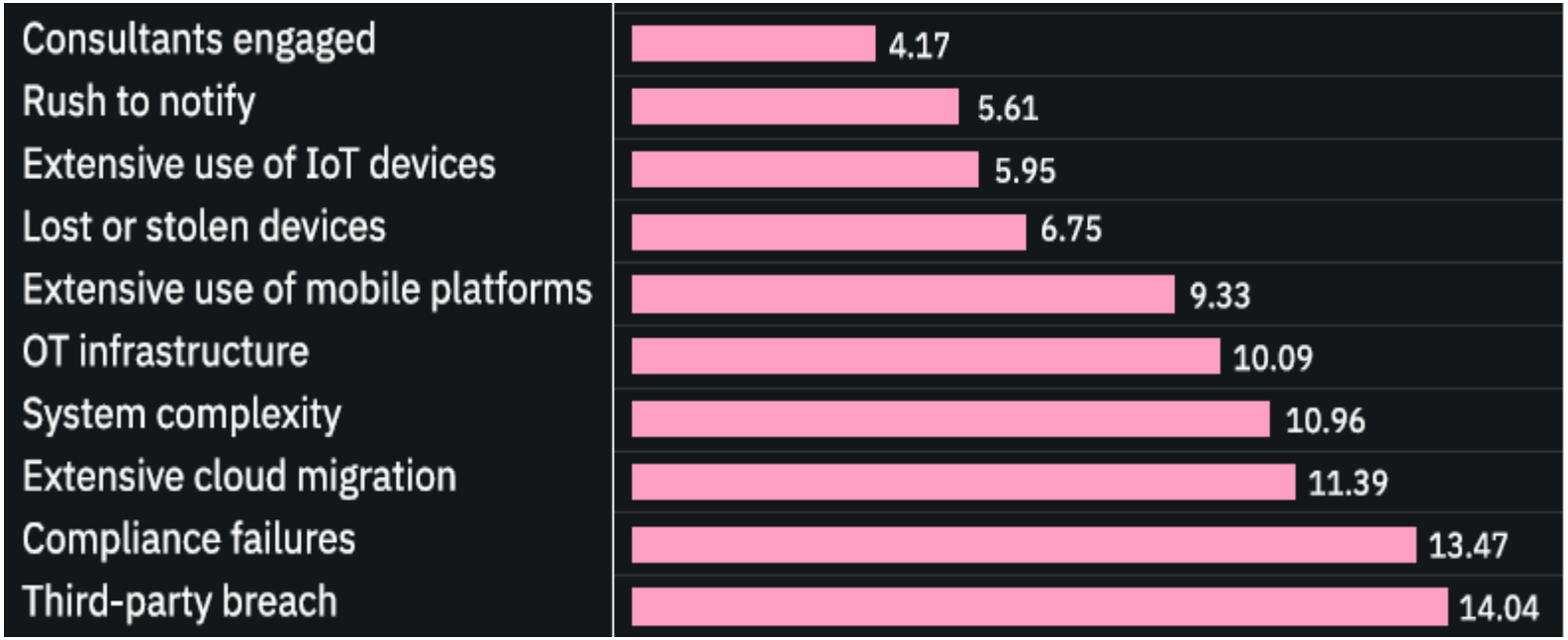
Cyber Defense: Decrease Costs



- Study by IBM and Ponemon Institute LLC

© 2019 BAIRD HOLM LLP

Cyber Defense: Increasing Costs



- Study by IBM and Ponemon Institute LLC

© 2019 BAIRD HOLM LLP

© 2019 BAIRD HOLM LLP

H.R. 7898

- Signed into law – January 3, 2021
- If organization can demonstrate that
  - for prior 12 months
  - Had recognized security practices
    - NIST / CSA of 2015 / other statutory recognized
- May
  - Mitigate fines
  - Early termination of audit
  - Mitigate remedies

© 2019 BAIRD HOLM LLP

Questions?

Disclaimer: This presentation is provided as a public service for informational, educational, or reference purposes. It is not designed to give individual advice. It is not legal advice or a substitute for legal advice. It does not create a lawyer-client relationship. Do not attempt to solve individual problems based upon the information contained in this presentation. Please seek the advice of an attorney for advice on all legal matters. No endorsement, warranty, or claim is made with respect to this presentation.

© 2019 BAIRD HOLM LLP

Thank You

Robert L. Kardell
BKardell@BairdHolm.com
www.BairdHolm.com

© 2019 BAIRD HOLM LLP