Cybersecurity in the Retirement Plan World

Duane Gran

Blue Ridge ESOP Associates


NAH, I'M NOT WORRIED ABOUT CLOUD SECURITY. MY STORED DATA IS SO DISORGANIZED THEY'D NEVER BE ABLE TO FIND ANYTHING!
© D.Fletcher for CloudTweaks.com

Some scary facts

- 41% increase in phishing volume in 2017 Q2
- 88% of those attacks targeted five industries:
  - **Financial institutions**
  - Online services
  - Payment services
  - Cloud providers
  - E-mail providers

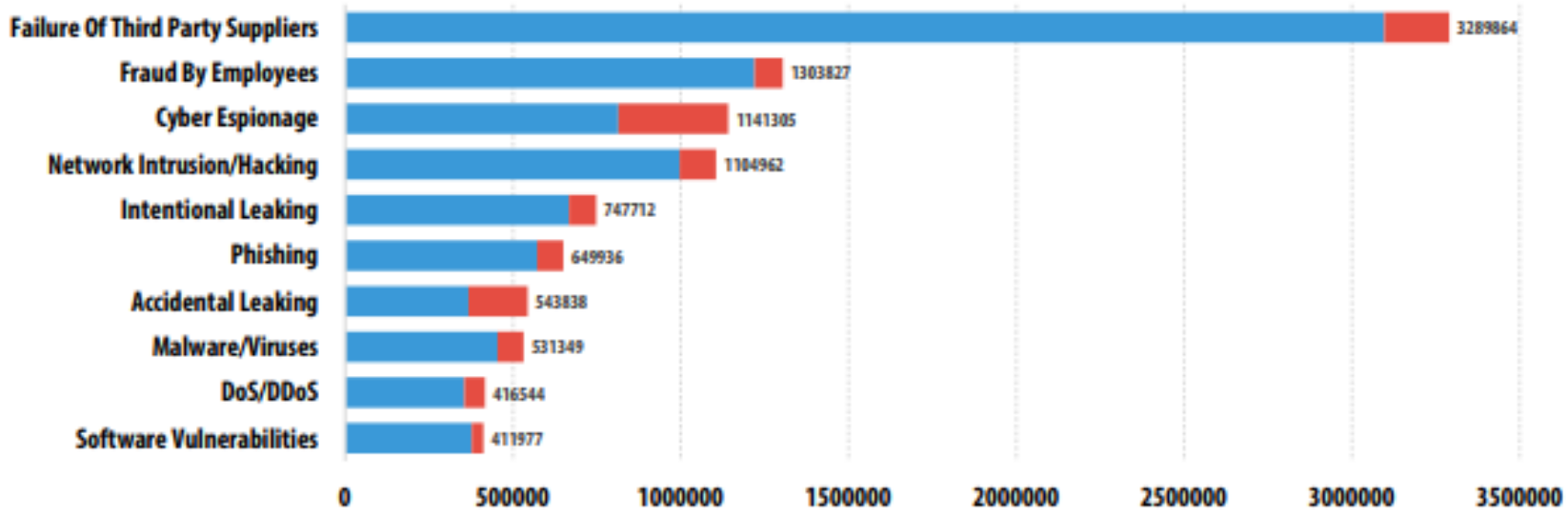
Source: Phishlabs 2017 Q2 report

Security breaches are expensive

- 90% of businesses in a Kaspersky survey admitted to having a security incident and 46% of them lost sensitive data as a result.
- Average remediation cost is $550,000 for enterprises and $38,000 for small businesses
- Indirect costs from reputation damage ranges from tens of thousands to over $200,000 per incident.

Cost of security incidents by type

Total financial impact of data breaches depends on the type of the incident. When we asked businesses, to attribute a security breach to a certain cause and estimate an amount of loss, we were able to pinpoint the most 'expensive' types of incidents.



Total impact of security incidents by type for enterprises

How is it happening?

Figure 3. What was the root cause of the data breaches your business experienced?
More than one choice allowed

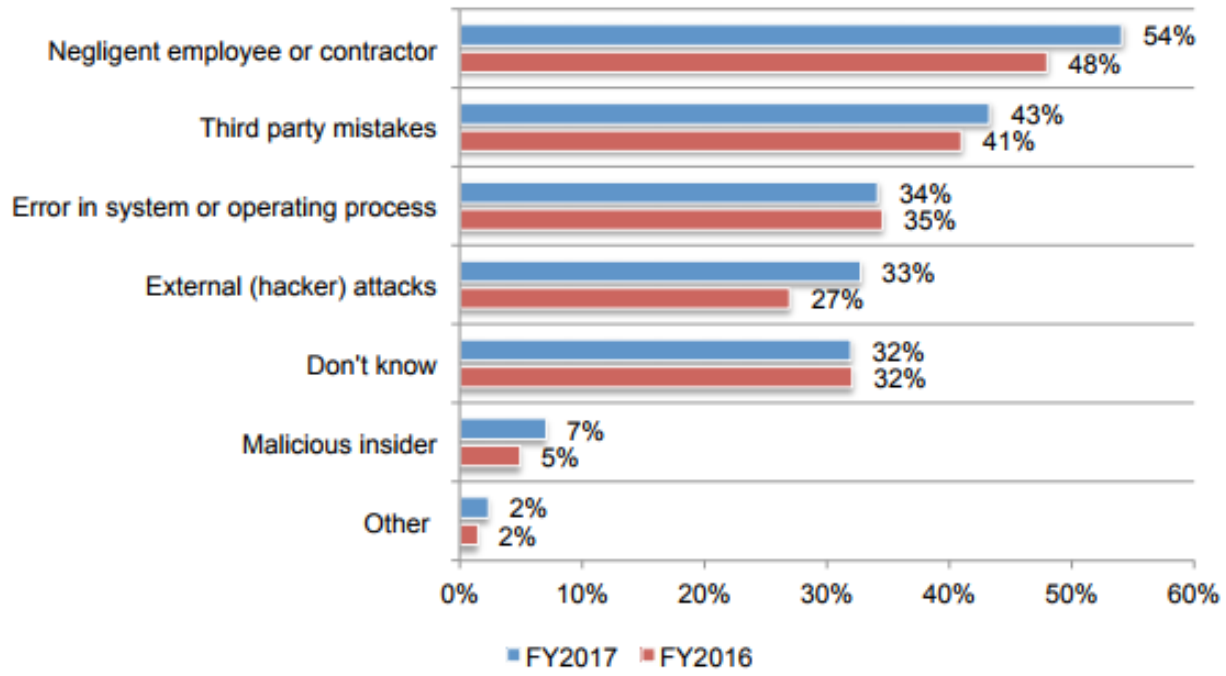
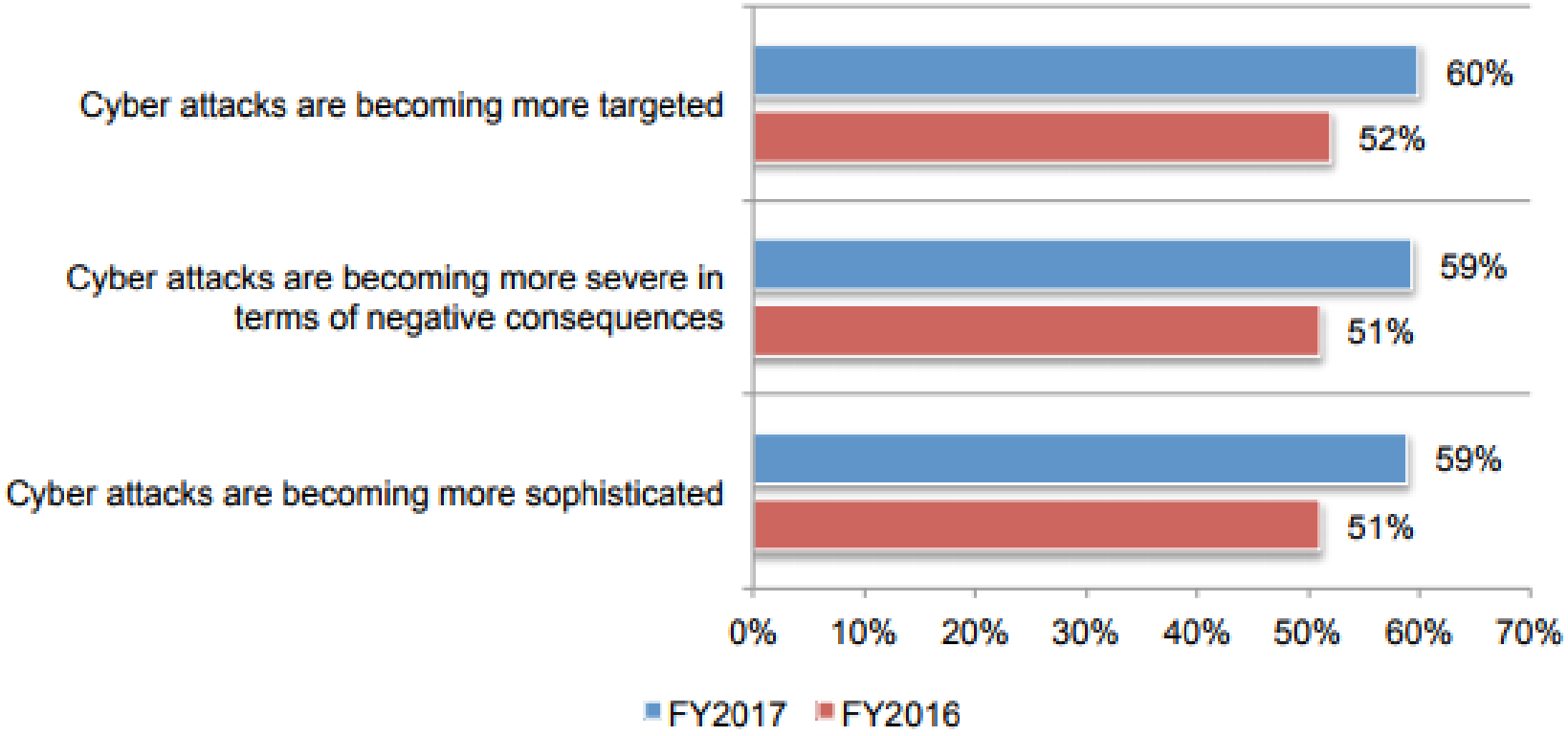


Figure 5. Perceptions about cyber attacks against their companies
Strongly Agree and Agree responses combined



Regulatory environment

- Nearly all states have similar, but differing, security breach notification laws.
- Forefront of these laws was CMR 17 from Massachusetts in 2010
- Federal Privacy Act of 1974 only impacts recordkeeping in the federal government
- H.R. 3806: Personal Data Notification and Protection Act of 2017 (in committee)

Insurance options

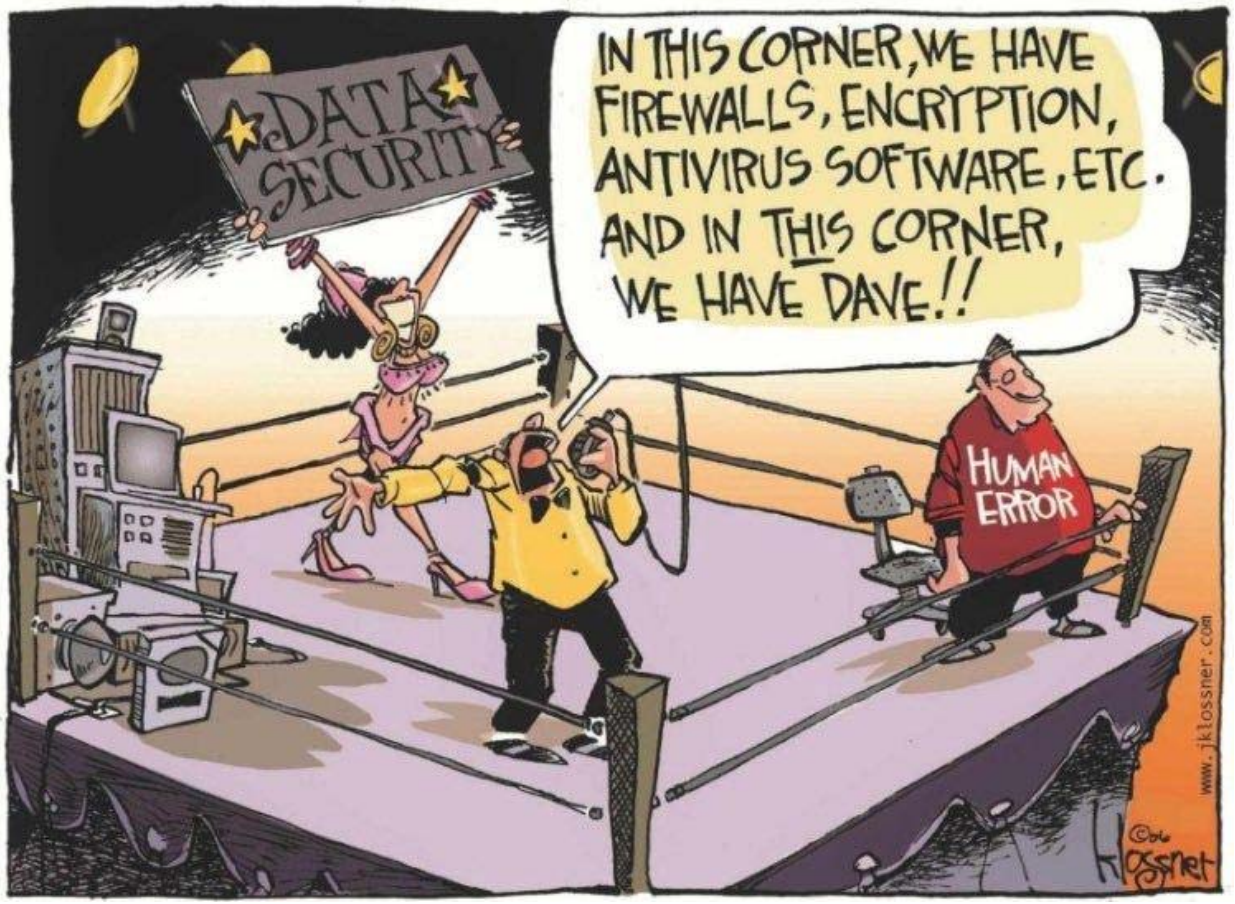
- Cyber Liability Insurance is common
- Policies cover costs for credit monitoring
- Naturally, no recourse for reputation damage
- Watch out for “human error” exception clauses because at heart every security incident is traceable to human error
- As an industry, not capable to price IT security risk on a per client basis

The bad news

- Threats are increasing
- Financial services are in the cross hairs of organized crime
- Error is costly
- Regulation is a confusing patchwork, insurance incomplete
- Third parties are often the weak link

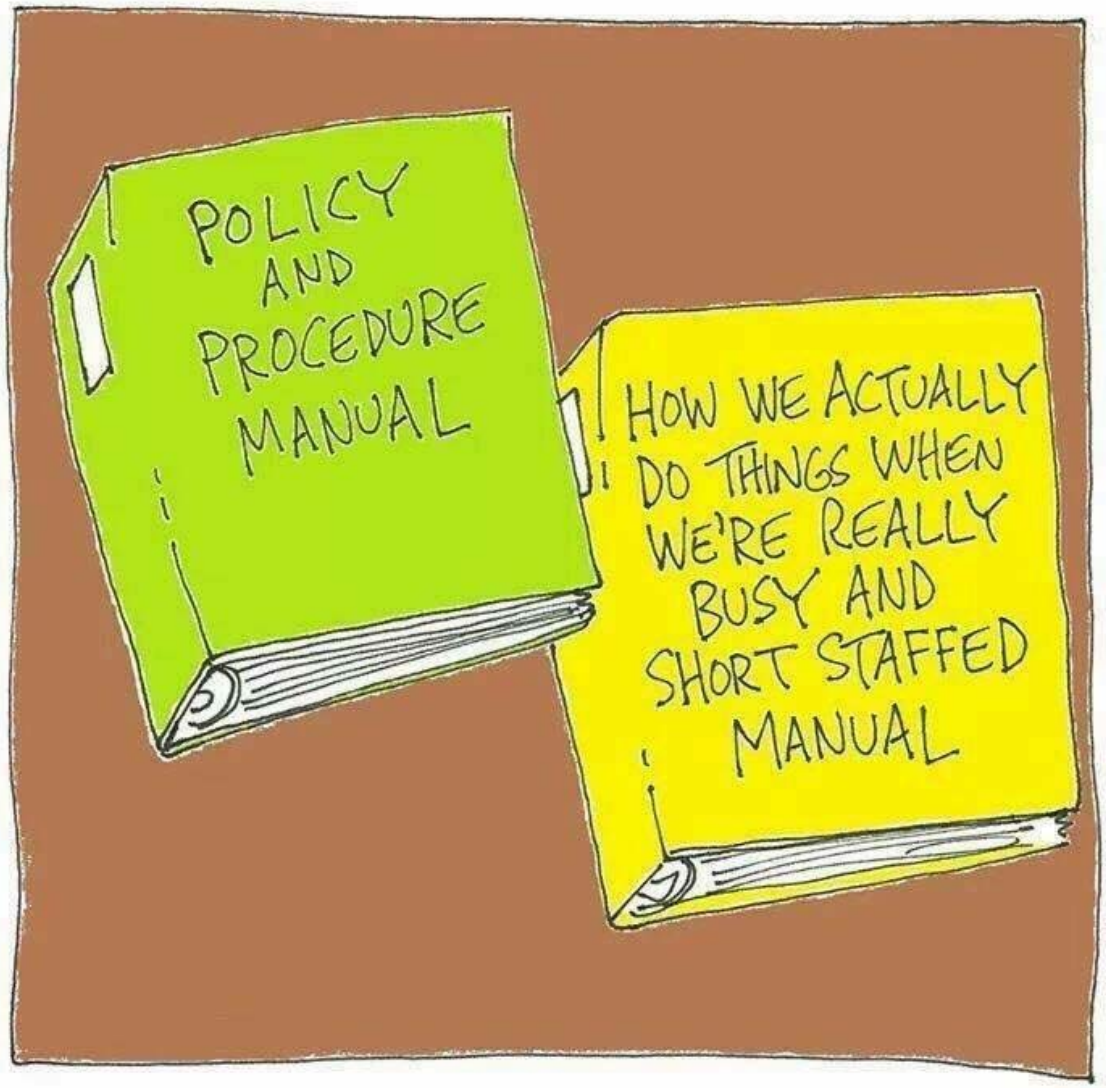
The good news (yes, there really is some)

- 90% of companies get attacked with 3 year old vulnerabilities (Fortinet Q2 2017 Global Threat Landscape report)
- Automatic updates are increasingly the norm for computer systems
- Vendors are recognizing the risk and factoring in security updates to their ongoing support. Medical industry particularly in rapid change mode.
- No one in 2017 should be surprised when you ask them to justify and explain how they will safeguard sensitive data


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 JKlossner

Practical things that improve IT Security

- Regular and automatic updates for operating systems and apps
- Password expiration policies
- Two factor authentication for sensitive applications
- Up to date virus scanning solutions
- Decommission old equipment that isn’t actively supported


POLICY AND PROCEDURE MANUAL
HOW WE ACTUALLY DO THINGS WHEN WE'RE REALLY BUSY AND SHORT STAFFED MANUAL

Things you always wanted to ask your vendor

(but were afraid to ask)

- Do you have a documented Security Program?
- Do you conduct criminal background screening for new hires?
- Do you provide security awareness training for staff?
- Describe your backup and disaster recovery plan
- What is your retention policy?
- How are physical and electronic records destroyed
- What forms of encryption are used and where is it used?
- How is employee access granted and revoked?

Security “smells” to watch for

- The website uses SSL, so it is secure
- Indications that they have purchased their security
- One person responsible for security instead of shared goal
- They wouldn’t know if they were compromised
- They have never had a security or privacy incident