Privacy and Data Breaches

CLS Compliance Conference

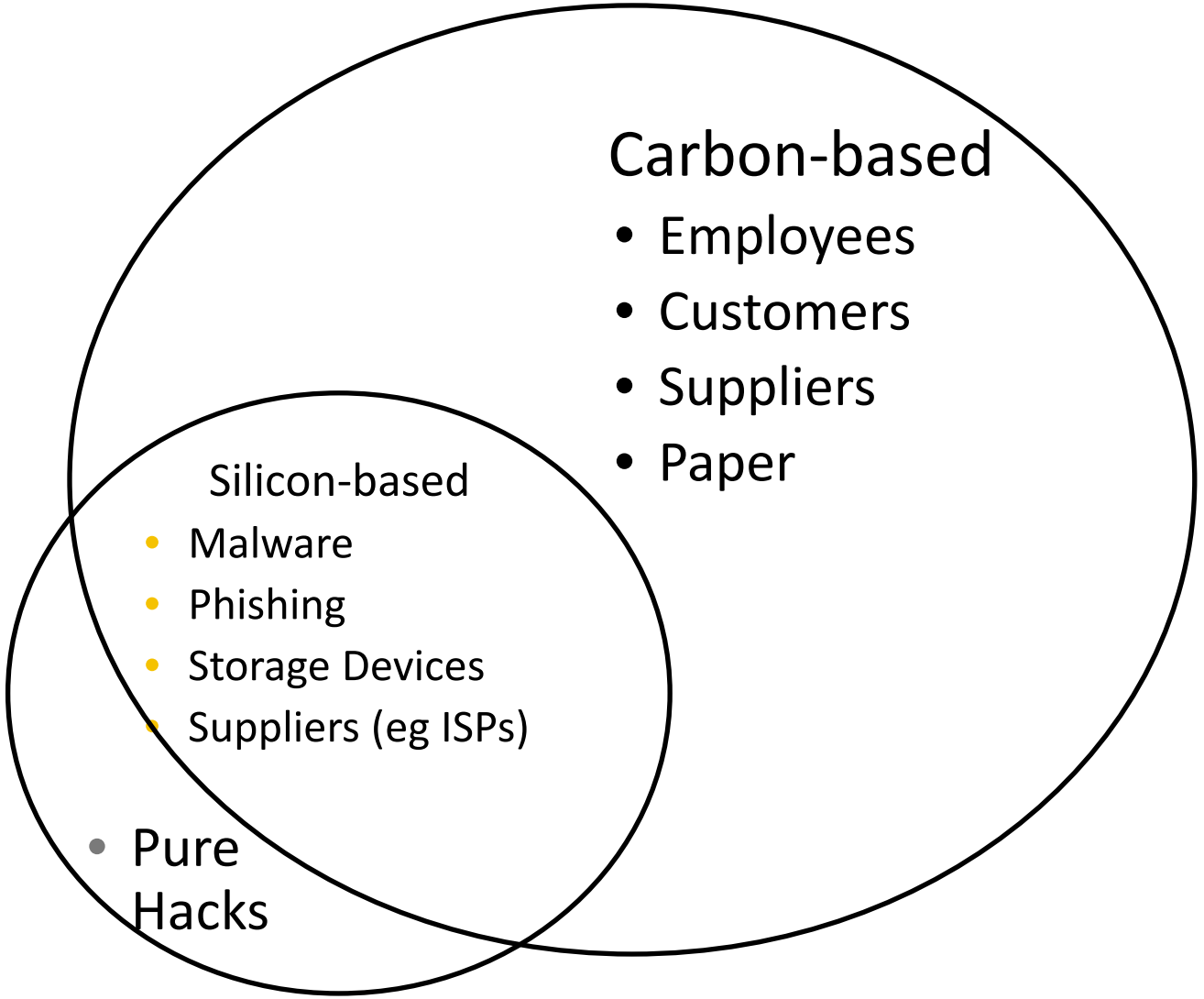
Tuesday, December 1st, 2015

Wayne Bolton, Edward Jones

Larry Boyce, Sutton Boyce Gilkes Regulatory Consulting Group Inc.

Karen Burke, BMO Financial Group

The Risks


Carbon-based
• Employees
• Customers
• Suppliers
• Paper
Silicon-based
• Malware
• Phishing
• Storage Devices
• Suppliers (eg ISPs)
• Pure Hacks

UK Federation of Small Business Survey: SMEs and Cyber Breach

- Security breaches up (scale and cost doubles since 2010)
- 11% changed nature of business due to worst breach
- 71% of SMEs suffered a security breach
- Median number of breaches: 4
- Average cost of worst security breach: £75-311, 000 (£65 – 115,000 in 2010)
- Malicious software is the fastest growing driver of security breaches, 60% of SMEs on the receiving end, up from 36% in 2010

Cyber Sleep

- 66% don’t think they are open to cyber attack
- Only 16% had improving cyber security as top priority
- 22% think small businesses are not a target
- 26% think only those taking payment online are at risk
- 24% think cyber security is too expense
- 22% don’t know where to start

Could it happen to you?

Response of 101 senior Silicon Valley executives to the question:
Could the Sony hack happen to your company?

Yes: 74%

"Anyone who thinks otherwise is deluding themselves"

- Dev Ittycheria, President and CEO, MongoDB

No: 26%

The Atlantic, Nov/15

Top 10 tips

Cybersecurity

- Combination of security protection (anti-virus, firewalls, etc.)
- Regular security updates on software and hardware
- Resilient password policy
- Secure wireless network
- Clear internet, email and mobile procedures
- Staff training and background checks
- Regulatory security risk assessment
- Regular security testing
- Check provider credentials
- Backup and disaster recovery

Privacy

- All of the cybersecurity tips
- Regular inventory updates; software, hardware and hard copy
- Secure destruction process
- Secure wireless network
- Clear access, movement, copying and retention procedures
- Staff training and background checks
- Regular risk assessment
- Regular testing (all locations)
- Check supplier credentials
- Breach management protocol

Breach Preparedness

- Start with an Organizational Review
- Strive for a mature privacy protection framework
- A mature privacy protection framework will make you both more protected from and more prepared for a breach when it does occur

Organizational Review

- Objectives and goals of your data framework, including risk appetite
- Policies and procedures
- Employee training
- Personal information and data, including data classification
- Collection, retention, use, processing and disclosure of personal information
- Systems and processes, including data flows
- Legal requirements that the organization must meet domestically and in other jurisdictions
- Vendor management
- Cloud
- Data Transfer
- Privacy risk identification, measurement, mitigation, monitoring and reporting
- Safeguarding data and personal information
- Gap analysis
- Incident management – breach identification and reporting, impact assessment, breach response team, investigation, stop the breach, breach remediation, breach prevention

Handling a breach
Scenario #1

Customer A received the monthly statement of Customer B, containing personal information of Customer B.

Handling a breach
Scenario #2

A courier bag is stolen, containing hundreds of credit card applications.

After the Breach

Consequences of the Breach:

- Impacted customers
- Regulators
- Media, including social media
- Call centre
- Other offerings, like credit monitoring
- Litigation or class action
- Post mortem and framework improvement
- Others?

Key takeaways

- Integrative approach: review activity relating to data safety should be viewed as key to the organization's larger risk management strategy
- Regulators' perspective: regulators view your suppliers and service providers, as well as their subcontractors, as a mere extension of you
- Modern economic and social context: tension between the rights of individuals to control their personal information and the need of a modern society and economy to function optimally both within and between jurisdictions
- Privilege: Give it proper consideration
- Documentation: Ensure a documented data governance plan with steps for on-going review
- ISO 27018: Code of practice for PII protection in public cloud acting as PII processors
- Digital Privacy Act: Regulations to come on reporting breaches of real risk of significant harm
- CASL: Privacy right of action to come into force in 2017

What's your breach learning or helpful hint?

Q & A

Thank you