RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: PNG-T07

Lessons Learned from Cybersecurity & Data Protection Roundtable: Role of GC

Natasha G. Kohne

Partner

Akin Gump Strauss Hauer & Feld LLP

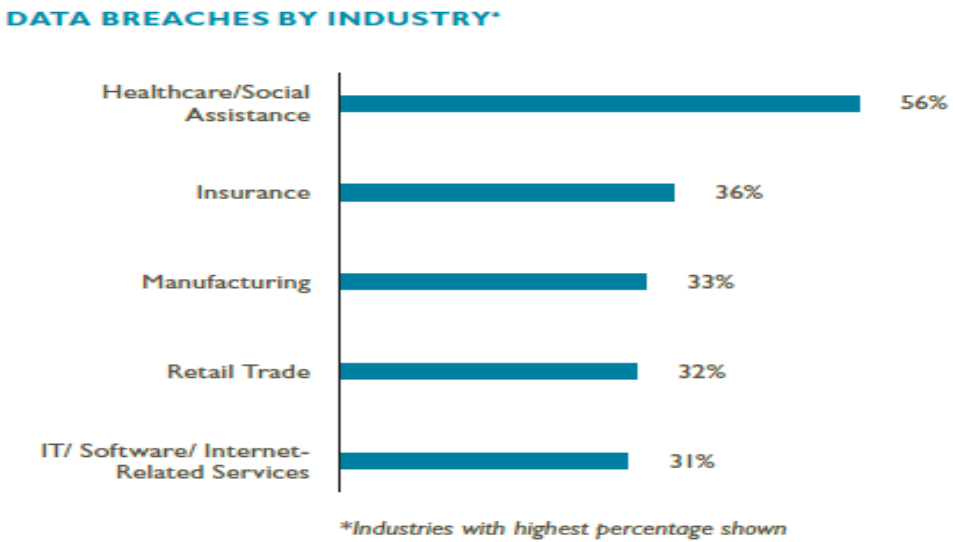
#RSAC

Statistics —What keeps you up at night?

- Cybersecurity and privacy are the leading issues that keep in-house counsel up at night.
- The Center for Strategic and International Studies estimates that “the likely annual cost to the global economy from cybercrime is more than US 400 billion.”
- One in three in-house counsel surveyed to have experienced a data breach at their company.
- The Association of Corporate Counsel (ACC) set out to generate the most comprehensive report of its kind and surveyed GCs and CLOs from 887 organizations in 30 different countries— an unprecedented record number of in-house counsel:
  - 50% of GC/CLOs want to increase their roles and responsibilities when it comes to cybersecurity.
  - 57% expect their department roles to increase in the coming year.
  - 56% of GC/CLOs say their company is allocating more money to cybersecurity than one year ago and that their legal department spend has increased as a result of company focus on cybersecurity.

Source: ACC’s The State of Cybersecurity Report: An In-house perspective

Statistics— Data Breach By Industry



"I wish we had done a better job at educating employees on cybersecurity issues, how to recognize and what to do and to become more informed on various ways that data breaches occur and proactive ways that could eliminate or reduce exposure."

Source: ACC's The State of Cybersecurity Report: An In-house perspective

Lessons Learned— Data Breaches

Preparation → Detection and Analysis → Containment and Remediation → Post-Incident Activity

- **Preparation**
  - Forensic firm (e.g., pre-engage, interview, revisit, oversight) (see casino case)
  - No alternative communication method
  - No data mapping – where are “crown jewels” and sensitive information
  - No retained counsel skilled in relevant computer crime
- **Detection and Analysis**
  - 72 hour notification once “discovered” (e.g., EU GDPR)
  - No prior analysis of “Reasonable Security” (e.g., CA AG)
  - Technical pitfalls:
    - Lack of understanding of enterprise computer environment
    - Lack of log files to determine date of breach event
    - Security controls not targeted to greatest risks
    - Lack of relevant network and host-based detection capabilities

Example: Oversight of Forensic/Auditing Firms

- Trustwave Lawsuit
  - In 2013, a casino operator suffered a security breach where malicious hackers penetrated its payment card systems.
    - Trustwave investigated the incident, and informed the breach was contained.
    - A few months later, Ernst & Young, in the course of penetration testing, found suspicious activity associated with malware that Trustwave was supposed to have removed.
    - Casino operator then suffered a second breach.
  - In January 2016, the casino operator sued Trustwave, alleging that it failed to properly investigate and contain the payment card breach. The complaint alleges that Trustwave misrepresented its ability to perform an adequate investigation, failed to identify the true source of the breach, and falsely assured the casino operator that the breach had been contained.

Affinity GAMING

Trustwave®

- Conflicts of Interest
  - Third party has strong interest to ensure reasonable security measures are in place.
  - Best practices include swapping out auditors every few years (duration can vary).

Lessons Learned— Data Breaches

Preparation → Detection and Analysis → Containment and Remediation → Post-Incident Activity

- **Preparation**
  - Forensic firm (e.g., pre-engage, interview, revisit, oversight) (see casino case)
  - No alternative communication method
  - No data mapping – where are “crown jewels” and sensitive information
  - No retained counsel skilled in relevant computer crime
- **Detection and Analysis**
  - 72 hour notification once “discovered” (e.g., EU GDPR)
  - No prior analysis of “Reasonable Security” (e.g., CA AG)
  - Technical pitfalls:
    - Lack of understanding of enterprise computer environment
    - Lack of log files to determine date of breach event
    - Security controls not targeted to greatest risks
    - Lack of relevant network and host-based detection capabilities

Example: Cybersecurity Standards/ Framework by Region

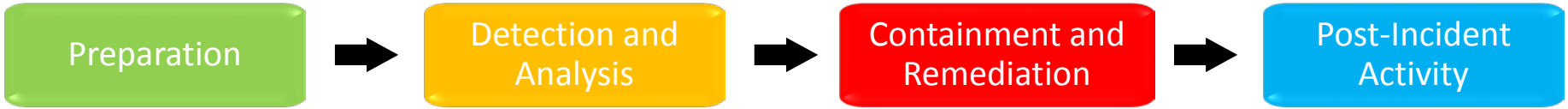
	U.S.	Canada	EMEA	Asia Pacific
	672	35	50	92
NIST	14%	6%	4%	1%
ISACA	3%	3%	6%	4%
SSAE 16	14%	9%	6%	1%
Six Sigma	2%	0%	2%	3%
SANS Critical Security Controls	2%	0%	0%	3%
ISO 177799 / 27001	13%	11%	30%	15%
COBIT 5	1%	0%	6%	2%
SSE-CMM	1%	0%	0%	1%
OWASP	1%	0%	0%	1%
Other—Please specify	5%	0%	2%	2%
None	5%	3%	10%	10%
Unsure	59%	74%	52%	68%

Source: ACC's The State of Cybersecurity Report: An In-house perspective

Example: California Attorney General: 20 "Minimum Level" Controls

Inventory of authorized and unauthorized devices	Inventory of authorized and unauthorized software	Security configurations for mobile devices, laptops, workstations, and servers	Continuous vulnerability assessment and remediation	Controlled use of administrative privileges
Maintenance, monitoring, and analysis of audit logs	Email and web browsing protection	Malware defenses	Limitation and control of network ports, protocols, and services	Data recovery capability
Secure configurations for network devices such as firewalls, routers, and switches	Boundary defense	Data protection	Controlled access based on the need to know	Wireless access control
Account monitoring and control	Security skills assessment and appropriate training to fill gaps	Application software security	Incident response and management	Penetration tests and red team exercises

Lessons Learned— Data Breaches



- **Containment and Remediation**
  - Improper evidence collection/preservation
  - No strategy regarding privileged communications
  - No communications strategy (e.g., employee or investor level, public statement, etc.)
- **Post-Incident Activity**
  - Forensic analyst reports (one draft/tone/language)
  - Lack of follow-up on recommendations
  - No understanding of legal obligations for notifications and multi-jurisdictional/multi-regulator cases
  - How to continue to operate with servers or certain aspects of business down

Example: Is GDPR Applicable to You?

- Applies to any controller or processor of EU citizen data
- Applies to most businesses selling to or monitoring EU citizens
- Includes online activities of non-EU companies
- Reaches more third-party technology providers
- Major impact on the cloud industry
- Expands personal data definition, e.g., adds genetic and biometric
- Many companies will now have to appoint a data protection officer

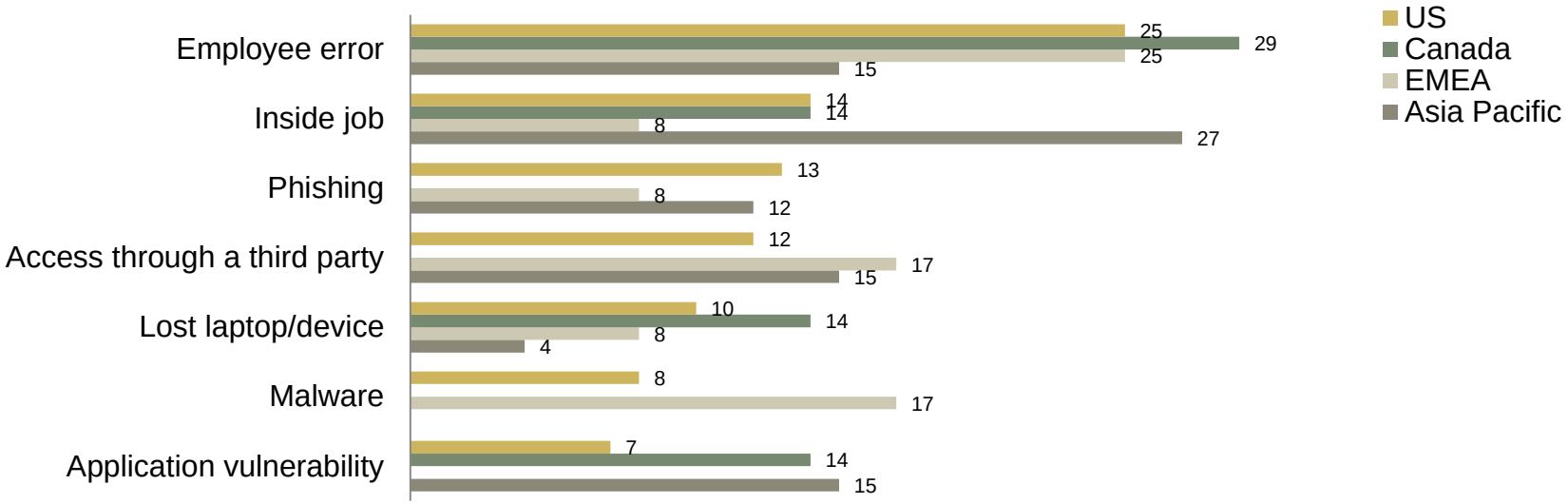
Insider Risk -- Vendor Management

Insider Risk -- Vendor Management

- Implement written vendor policies & procedures
- Conduct due diligence at pre-contractual stage (including risk assessments)
- Employ principle of limited access (see Target example)
- Implement technological safeguards (encryption, access controls)
- Negotiate protective contractual provisions
  - Attestations of security
  - Audit rights
  - Notice requirements and ownership
  - Limit downstream data transfers
  - Termination procedures
  - Indemnification provisions
  - Insurance requirements
- Ensure effective processes for monitoring, reviewing and auditing third-parties and related follow-up
- Training by firm of third-party vendors
- Properly terminate contractual relationship

Insider Risk – Employees

CAUSE OF BREACH BY REGION*



Source: ACC's The State of Cybersecurity Report: An In-house perspective

Insider Risk -- Morgan Stanley (June 2016)

- A former employee of a Morgan Stanley indirect wholly-owned subsidiary, MSSB, accessed and downloaded customer PII from two firm portals to his personal storage device. The device was then hacked by a third party, which posted portions of the information to three different websites
- On June 8, 2016, the SEC found MSSB's policies and procedures were not reasonably designed to meet the objectives of the Safeguards Rule by failing to include, for example:
  - reasonably designed and operating authorization modules for the Portals that restricted employee access to only the confidential customer data as to which such employees had a legitimate business need
  - auditing and/or testing of the effectiveness of such authorization modules
  - monitoring and analysis of employee access to and use of the Portals
- MSSB was fined a $1 million civil money penalty and ordered to cease and desist

Insider Risk -- Special Attention for Employees

- **Insider threat – employees**
  - Weak link in organizations
  - Lack of culture of security
  - Conventional practices involving security training not effective
- **Cutting-edge tactics to engage employees and develop culture of security**
  - Need-to-know access
  - Accountability and responsibility
  - Revisit hiring practices
  - Integrate into evaluation and compensation process
  - Monitoring employees to the extent permitted by law
  - Monitoring or auditing authorization modules

M&A Due Diligence

- **Initial considerations:**
  - Who's your target (e.g., retail, health, financial, defense, etc.)?
  - What type of information/data will you be acquiring (e.g., PII, IP, PHI, etc.)?
- **Due Diligence (sample questions):**
  - What are the current data security and privacy practices of the target?
  - What technical controls are in place?
  - What is the existing cyber and privacy policy framework, including policies and procedures? How often are they updated? Are they followed?
  - What is the governance structure of the target?
  - Did the company perform risk assessments? Were the gaps addressed?
  - How many breaches has the target experienced in the past? How were they addressed? Were there any public disclosures? Were there investigations or litigation?
  - What are the target's greatest security concerns?

M&A Due Diligence (cont'd).

- Management Questions
- Due Diligence Report
- Bank Financing
- Upon purchase, address red flags
- Ensure proper integration into enterprise-wide system

Next Steps

- Immediate:
  - Map your crown jewels
  - Know your legal and technical requirements/standards
  - Perform cyber and data protection diligence on new key contractual third-parties
- Medium-Term (3 months):
  - Develop and solidify relationships with forensic and legal counsel
  - Identify multi-disciplinary incident response team
  - Run a Table Top Scenario
  - Identify third-party contracts up for renewal to determine renegotiations of cyber and data protection provisions/consider renegotiation of key contracts
  - Review compliance framework and identify gaps

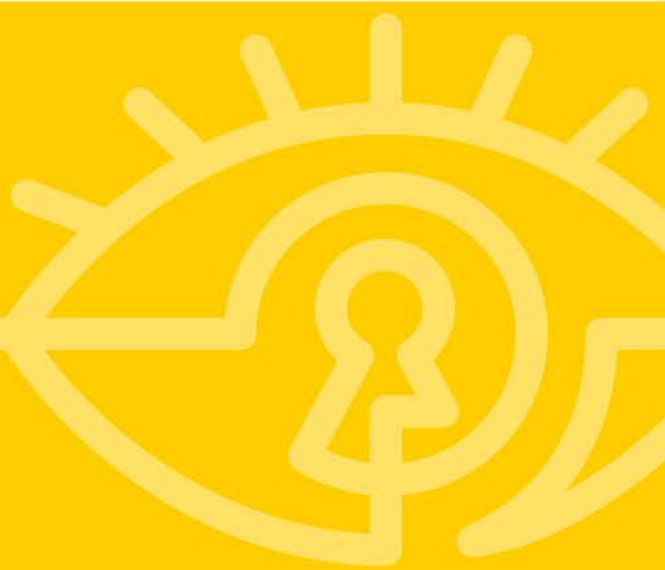
Next Steps

- Longer-Term (6 months):
  - Follow-up on gap analysis
  - Integrate security culture into routine business activities (evaluations, incentives, etc.)
  - Annual assessment of cyber policies and procedures and training

Developing a Framework for Cyber Protection

Companies, including Akin Gump, work with companies to develop / advise on:

1. **Tailored Written Policies and Procedures** – governance, risk identification, access, surveillance and testing
2. **Incident Response Plans** – alert thresholds, escalation, law enforcement and client notification, incident investigation and loss allocation
3. **Operational Protocols** – data intake/flow, vendor oversight, employee training, data protection and disclosures
4. **Due Diligence** – advise on M&A and other cybersecurity due diligence
5. **Breach Response** – identify the nature and scope of the intrusion, work with the IT team and experts to restore normal system operation, provide required disclosures and notices, and defend regulatory investigations and/or class actions



Questions?