Preparing for evolving cyber threats and regulations

Impacts of cybersecurity and data privacy on your business

October 28, 2019
Agenda

01 Introductions

02 What is cybersecurity?

03 Impacts of cyber crime

04 Evolving data privacy legislation

05 What can you do?
Introductions

Brian Nichols
Director – Risk, Internal Audit & Cybersecurity

Eric Wunderlich
Senior Manager – Risk, Internal Audit & Cybersecurity
Cybersecurity today

Today's digital world

Cybersecurity = Trust

Who are you?

What should you have access to?
Building a sustainable cybersecurity model

Balancing your efforts across all four dimensions will improve your cybersecurity program oversight.
How confident are you?

77% of CEOs and Boards are optimistic in their organization’s ability to cope with a data breach.

But only 33% are confident that high-value assets are adequately protected.
Impacts of cyber crime
Impacts of cyber crime

2/3 of cyberattacks are targeted at small and medium sized businesses.

191 Days
Average time to identify a breach.

32%
Chance of a C-Suite Executive being terminated after a breach.

77%
of organizations do NOT have a formal incident recovery plan.

$7.9M
Average cost of a data breach.

60%
of small and medium sized businesses will no longer exist 6 months after a breach.
The basic motives – know your enemy

Understanding the adversary's motivation is key to making the best cyber governance decisions.

**Warfare**
Disrupt, degrade, deny, destroy

**Espionage**
Unauthorized access to information

**Crime**
Commit fraud or theft of information

Adversaries' tactics, techniques & procedures (TTP), intel, and outcomes vary
Cyber threat trends

Focus on major trends but don’t lose sight of emerging threats
Cyber threat trends

Focus on major trends but don’t lose sight of emerging threats
Putting cyber crime into perspective

Cyber crime generates $1.5 trillion per year.

If cyber crime were a country, it would have the 13th highest GDP in the world.
Recent cyber attacks

DURING THE FIRST 6 MONTHS OF 2019

3,800+ publicly disclosed breaches

4.1 billion compromised records

3.2 billion of those records were exposed by just 8 breaches

TOP SOURCES OF DATA BREACHES

70% email
65% passwords

Source: Risk Based Security research 2019 MidYear QuickView Data Breach Report
Evolving data privacy legislation
Cybersecurity vs. data privacy
How are they related?

Privacy laws and regulations set the legal standards for what information should be protected; cybersecurity is the practice of protecting and ensuring that data is kept private.

Privacy cannot exist without cybersecurity
These privacy laws are just the tip of the iceberg

Privacy is global

United States
- CCPA – California Consumer Privacy Act (2018)
- COPPA – Children’s Online Privacy Protection Act (2000)
- Other U.S. state regulations

European Union
- GDPR – General Data Protection Regulation (2016)
- Privacy Shield
- E-Privacy (2002)
- EU Member Regulations

United Kingdom
- Data Protection Act (2018)

Canada

China

Australia
- APP – Australian’s Privacy Principles (1988)

Philippines
- Republic Act 10173 (2012)

India
- PDPB – Personal Data Protection Bill

Malaysia
- PDPA – Personal Data Protection Act (2010)

Brazil
- Brazilian Internet Act (2014)
- LGDP - General Data Privacy Law (2018) effective 2020

New Zealand
- Privacy Act (1993)

Canada

United States
- CCPA – California Consumer Privacy Act (2018)
- COPPA – Children’s Online Privacy Protection Act (2000)
- Other U.S. state regulations

European Union
- GDPR – General Data Protection Regulation (2016)
- Privacy Shield
- E-Privacy (2002)
- EU Member Regulations

United Kingdom
- Data Protection Act (2018)

Canada

China

Australia
- APP – Australian’s Privacy Principles (1988)

Philippines
- Republic Act 10173 (2012)

India
- PDPB – Personal Data Protection Bill

Malaysia
- PDPA – Personal Data Protection Act (2010)

Brazil
- Brazilian Internet Act (2014)
- LGDP - General Data Privacy Law (2018) effective 2020

New Zealand
- Privacy Act (1993)
**U.S. V. EU VIEWS ON PRIVACY**

Business-centric v. individual-focused

**United States view**

Businesses own the data they collect about individuals

**European Union’s view**

Individuals own the data about themselves and give businesses limited usage rights
Where we are today?

Zuckerberg defends Facebook in new data breach controversy

[LONDON] Facebook chief Mark Zuckerberg pushed back Wednesday against emails showing the social media giant offering Netflix and other popular apps preferential access to people’s data even...

'Tracking every place you go': Weather Channel app accused of selling user data

Most popular mobile weather app misled users who shared location information, say Los Angeles prosecutors in lawsuit

Facebook fined £8.9m by Italy for misleading users over data use

Alexa user accesses stranger’s chats

A man who requested access to the chats Amazon had recorded was sent audio files from a stranger.

Data breach complaints up 160% since GDPR came into force
Using GDPR as a template for privacy

<table>
<thead>
<tr>
<th>Key tenets of GDPR</th>
<th>Data subject rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Transparency</td>
<td>- Data access</td>
</tr>
<tr>
<td>- Purpose limitation</td>
<td>- Right to object</td>
</tr>
<tr>
<td>- Data minimization</td>
<td>- Data rectification</td>
</tr>
<tr>
<td>- Accuracy</td>
<td>- Restriction of processing</td>
</tr>
<tr>
<td>- Data deletion</td>
<td>- Data portability</td>
</tr>
<tr>
<td>- Security</td>
<td>- Right to erasure</td>
</tr>
<tr>
<td>- Accountability</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key tenets of CCPA</th>
<th>Data subject rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Transparency</td>
<td>- Data access</td>
</tr>
<tr>
<td>- Applicability</td>
<td>- Right to inform</td>
</tr>
<tr>
<td>- Categories of collected info</td>
<td>- Right to opt-out</td>
</tr>
<tr>
<td>- Disclosures of personal information</td>
<td>- Right to delete</td>
</tr>
<tr>
<td>- Data deletion</td>
<td>- Data rectification</td>
</tr>
<tr>
<td>- Security</td>
<td>- Restriction of processing</td>
</tr>
<tr>
<td>- Accountability</td>
<td>- Right to erasure</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What can you do?
Focus on data classification and governance

Identify
- Catalog information assets within the area under review
- Compare against enterprise-wide or departmental data inventory

Locate
- Confirm where information assets and data resides
- Be aware of interfaces, backups and archives

Classify
- Assess criticality of information assets and data to the area under review
- Evaluate the groupings or categories of data (customer data, consumer data, publicly available, credit card data, etc)

Value
- Consider regulatory compliance impacts as well as competitive advantage (trade secrets)
- Evaluate processes and controls in place to protect the data in comparison to the importance and criticality of the data
Review data flow mapping

Provide assurance on the **data flow mapping process** and ensure mapping considers all key flows.

- What data items are being collected? In what formats?
- How is the data being collected and transferred?
- What are the reasons for capturing the data?
- Are data retention periods documented?

Be sure to review **data privacy practices in cloud processing** as well.

- Does the organization maintain records of data processing in the cloud?
- Do cloud service provider contracts include relevant clauses and requirements for data protection in line with GDPR and other privacy regulations?
- Have cloud service provider’s data protection practices been reviewed?
Evaluate security controls and identify gaps

- Utilize control standards (NIST CSF, NIST 800-53, ISO 27001, SANS CIS) where appropriate to benchmark current controls
- Review and evaluate the extent of encryption on all devices, including laptops and mobile phones
- Review access management policies and controls to ensure logical access is based on legitimate and defined business needs
- Review patch management processes and the way in which patches/updates are identified, evaluated, and installed
- Evaluate physical security controls for data centers, server rooms, as well as overall office spaces and buildings
- Conduct vulnerability scanning and penetration testing to identify vulnerabilities and assess the organization's ability to detect and respond to threats
Evaluate resiliency to a cyber attack

- Ensure management is planning today
- Organizations with a regularly tested incident response plan are better suited to weather the storm and minimize impact to reputation and loss of customer confidence.

**Cyber incident response plan**

Ensure the plan(s) include clear roles, responsibilities, and contact information. Also, consider testing this plan regularly (at least once a year) to ensure people are aware of their roles and responsibilities.

**Business continuity and disaster recovery plans**

Ensure the plan(s) include clear roles, responsibilities, and contact information. Evaluate whether management has adequately identified how long the business can survive without a system, application, or data. Also, consider testing this plan regularly (at least once a year) to ensure people are aware of their roles and responsibilities.

**Engage outside assistance and trusted third parties**

Evaluate whether additional expertise or bandwidth is needed to assist with cybersecurity or data breach response. This includes outside legal counsel, public relations, and cyber response teams.
Be aware of who you do business with

Business today is not performed in a silo, most organizations have multiple business partners that they use to perform specific business functions. These third parties introduce risk to your business that you may not even be aware of.

- **Identify the third party vendors/suppliers** that have a business relationship with your organization. Evaluate the risks that the vendor potentially poses to the organization (e.g. do they process payroll information?, do they have access to your network?, do they send marketing material to your customers?) and ensure appropriate controls are in place.

- **Ensure management performs risk assessments** on the most critical third party vendor relationships and validate that contractual agreements have security and privacy requirements clearly identified in the agreement.

- If the vendor provides an IT service (such as outsourced payroll processing), validate that the vendor obtains a third party assessment on an annual basis **SOC 1 or SOC 2 reports** (System and Organization Controls). Obtain and review these assessments for any internal control matters.
Help to build a security aware culture

Protecting your organization is not all about the technology, people are a major contributing factor to whether you will suffer a data breach. Users are being targeted every day and many organizations are falling victim to malware or ransomware infections due to the lack of cybersecurity awareness of their end users.

- **Ensure employee onboarding** includes discussion on security expectations (e.g. not sharing passwords, locking your computer when you step away, protecting sensitive company information). Management should also provide new employees the information security policy to review and sign-off that they have actually read the policy.

- Participate and support **ongoing security awareness** through internal marketing emails, posters, and an annual security refresher.

- Additionally, due to the increased use of phishing to compromise organizations, Internal Audit should consider **phishing campaigns** to test users and increase their awareness of the threat vector.
Questions? Connect with us

Brian Nichols
Director – Risk, Internal Audit & Cybersecurity
brian.nichols@bakertilly.com
+1 (972) 748 0496

Eric Wunderlich
Senior Manager – Risk, Internal Audit & Cybersecurity
eric.wunderlich@bakertilly.com
+1 (312) 729 8185
Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly Virchow Krause, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. © 2019 Baker Tilly Virchow Krause, LLP.