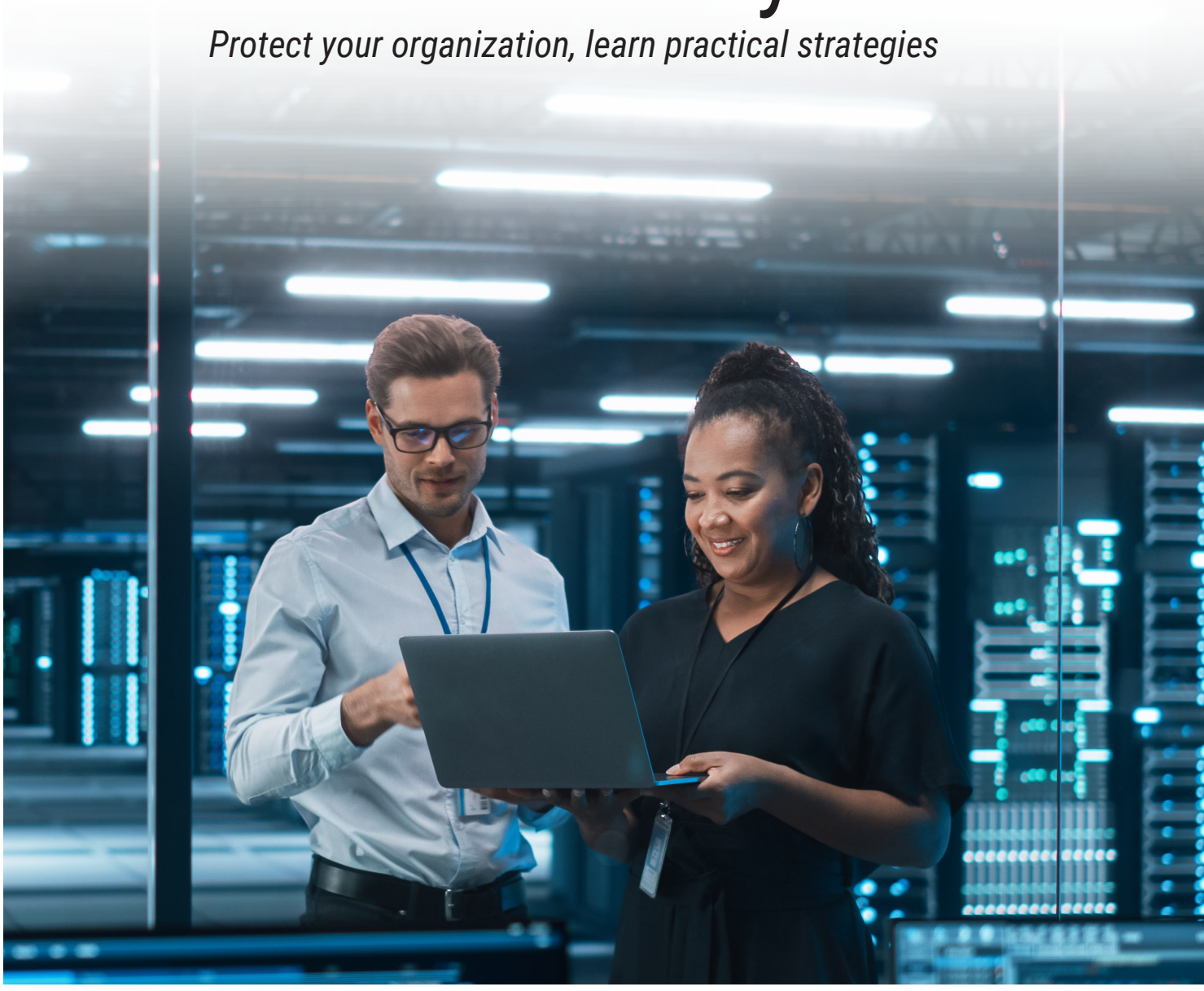
ACC Association of Corporate Counsel

Cybersecurity Toolkit for In-house Lawyers

Protect your organization, learn practical strategies



WHAT IN-HOUSE LAWYERS SAY ABOUT THIS TOOLKIT:

"It is an increasingly important field with which every in-house counsel should have some measure of familiarity. The good news is, if someone is hearing some of the guidance in this toolkit for the first time, it means that there is room to strengthen their defenses. And with every company that adopts positive cybersecurity practices, all corporations get a little safer as a result."

Bunny Smith, *Global Cybersecurity Counsel*, Yahoo!

Thank you to ACC members

The ACC team warmly thanks the global group of ACC members who shared in-house insight regarding this toolkit *(their input was personal and not on behalf of their organizations)*:

Abha T. Romkey
Vice President,
Corporate Legal Services
Emera

Lavonne Burke
Vice President Legal –
Global Security & Resiliency, Digital (IT) and AI
Dell Technologies

Bunny Smith
Global Cybersecurity Counsel
Yahoo!

Robert Kang
Professorial Lecturer
The George Washington University Law School
and former in-house legal executive

Jennifer K. Mailander
Vice President, Deputy General Counsel
Fannie Mae

Stephen H. Baird
Associate General Counsel
SITA

Kenny Goh
Senior Legal Counsel
Changi Airport Group

Wei Loong Siow
Legal Counsel & Data Protection Officer
Changi Airport Group

ACC thanks Jackson Lewis P.C. for their generous sponsorship of this toolkit and for the content they provided for this resource.

JacksonLewis

WELCOME

Cybersecurity remains a critical issue at all levels. Cyber threats are escalating, with data breaches and security incidents becoming more frequent, sophisticated, and harmful.

For many organizations, the challenge has been exacerbated by the shift to remote work and the expanding use of digital tools and AI. According to ***IBM's Cost of a Data Breach Report***, the average cost of a data breach globally in 2024 was USD 4.88 million, emphasizing the urgent need for enhanced protection measures and awareness.

This global issue affects every industry. It remains one of the top priorities for general counsel and chief legal officers, as reported again this year in ACC's latest ***Chief Legal Officers survey***. In-house lawyers play an essential role in helping their organizations protect themselves against these threats and respond to cyber incidents.

Designed for all in-house lawyers with a focus on cybersecurity, this toolkit offers practical insights and checklists to enhance your cybersecurity practices and to support your team in mitigating potential risks. A special thanks to all ACC members who contributed. Special thanks also to the Jackson Lewis P.C. law firm for their sponsorship and support by lending their thought leadership on these critical issues. Everyone's engagement is vital in addressing these challenges effectively and fostering a more secure digital environment.

As with all ACC resources, we are committed to keeping this toolkit up-to-date and relevant. Your feedback and suggestions are invaluable to help us to continually improve. Please share your thoughts with us at ***legalresources@acc.com***.

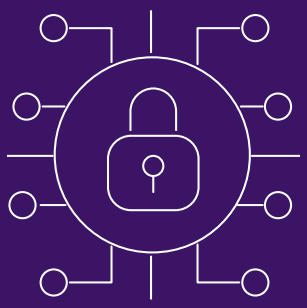
Thank you for your dedication to strengthening your organization's cybersecurity readiness. ACC is pleased to provide practical resources for global in-house lawyers to be effective, recognized, and successful.

Best regards,

Veta T. Richardson

PRESIDENT AND CEO
ASSOCIATION OF CORPORATE COUNSEL

JacksonLewis



Proud sponsor of the ACC Annual Meeting and sole sponsor of the ACC Employment + Labor Law Network.

Longtime provider of workplace and related services to leading single-site, multistate and multinational organizations.

Your partner for navigating and responding to cybersecurity threats and privacy compliance challenges.

Jason C. Gavejian

Principal + Privacy, Data and Cybersecurity Co-Leader

Berkeley Heights
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti

Principal + Privacy, Data and Cybersecurity Co-Leader

Tampa
Joseph.Lazzarotti@jacksonlewis.com

About Our Privacy, Data + Cybersecurity Practice Group

CONTENTS

ADDRESS CYBERSECURITY CHALLENGES

Learn and connect with global executives in legal departments, business, government, and academia. Explore best practices and real-world challenges with leading cybersecurity experts and technology solution providers.

ACC Foundation
Association of Corporate Counsel

2025 CYBERSECURITY SUMMIT

MARCH 24+25

University of California Los Angeles

REGISTER TODAY!

Gain More Cybersecurity Insight.

Read the ACC Foundation
State of Cybersecurity Report

DOWNLOAD NOW

Who is this toolkit for?

This toolkit is relevant for all in-house counsel who want to gain a baseline understanding of cybersecurity strategies or develop their cybersecurity in-house skills to **help their business understand and navigate these challenges**.

- Cybersecurity is likely an important part of your organization's risk profile, its assets protection, contractual relationships, and its regulatory landscape.
- Around the world, cybersecurity and data privacy laws with a global impact often present a complex regulatory patchwork that can be difficult to manage - to name a few, the EU General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the Australian Privacy Act, etc.
- General counsel and their team have a leading role to play in helping the business prepare and respond to cybersecurity challenges.
- This toolkit offers practical checklists and insights to help you be an effective leader in your organization's cybersecurity preparedness.

Where is this insight from?

The insight in this toolkit is mainly based on:

- Resources from the ***ACC Resource Library*** that the ACC team has found relevant;
- Thought leadership from law firm ***Jackson Lewis P.C.***; and
- The perspectives of ACC members, experienced in-house counsel who kindly shared input.

The Association of Corporate Counsel

- The Association of Corporate Counsel (ACC) is a global bar association.
- ACC promotes the common professional and business interests of in-house counsel through information, education, networking opportunities, and advocacy initiatives.
- The ACC community includes more than 46,000 members from around the world.
- ACC is invested in your success as an in-house lawyer, a General Counsel, or a Chief Legal Officer. ACC advocates for you to have a "Seat at the Table" and provides value with resources for your team to succeed.
- Are you an in-house counsel? ***Join us!*** Learn, connect with peers, and boost your career.

8 Key Points for In-house Counsel

1. **Assess your organization's cyber risk** in light of its business profile, third-party relationships, and risk tolerance.
2. **Prior to any attack, develop a practical incident response plan** with your specialist teams. This plan enables your organization to rapidly respond with pre-agreed decision-making rules and communication channels.
3. **Identify your cyber insurance needs** (coverage and amounts). If you have cyber insurance, know the requirements in the event of an incident.
4. **Communicate carefully** regarding incidents, internally and externally.
5. **Consider your approach for maintaining legal privilege.**
6. **Train employees** to recognize, prevent, and report cyber threats.
7. **Address key cyber risks in your contracts** with counter parties.
8. **Weave cybersecurity** into your company's approach to **AI tools.**

Fact Sheet

Here are five top-of-mind findings from the ***ACC Foundation State of Cybersecurity Report*** and the ***2024 ACC Chief Legal Officers Survey Report***:

1. **CLOs report cybersecurity threats** as a top issue keeping them up at night.
2. **Most chief legal officers** have cybersecurity-related responsibilities.
3. **More than 60% of companies** require cybersecurity training for **all** employees.
4. **Top breach-related concerns** are reputation, liability, and business continuity.
5. **Few legal teams report being "often" involved** in the company's third-party risk management.

Learn more

→ Read the findings from the latest ***ACC Foundation State of Cybersecurity Report***.

→ View the following checklists and the resource shortlists at the end of the toolkit.

CHECKLIST 1

Assess and Strengthen the Organization's Cybersecurity Practices

Get your organization ready to defend against cyber threats.

1. Conduct a cybersecurity risk assessment and identify gaps:

- Risk assessments can be conducted by **in-house specialist teams** and/or with **external consultants**.
- A risk assessment may represent a **significant undertaking.**
- **Inventory your organization's ecosystem.** Identify the "crown jewels" of your business, its most valuable assets that need protection against cyber threats.
- **Roadmap the current state** of your company's cybersecurity program - which may include components specific to the law department.
- Apply an **appropriate cybersecurity framework** to benchmark your findings. Here are examples of well-known frameworks:
  - The Center for Internet Security's ***CIS Critical Security Controls®***,
  - The International Organization for Standardization's ISO ***standard 27001***,
  - The US National Institute of Standards and Technology's (NIST) ***frameworks***,
  - The US Federal Financial Institutions Examination Council's ***Cybersecurity Assessment Tool***,
  - The ***UK GDPR Breach Response and Monitoring Guidance***,
  - The Australian Signals Directorate's ***Essential Eight***,
  - The Canadian Centre for Cyber Security's ***Cyber Security Skills Framework***.
- **Consider your business profile** (small vs. large, online vs. physical, etc.) in developing your assessment framework.
- **Consider your supply chain risks**, especially from key vendors that will increase your vulnerability and susceptibility to cyber incidents. *See **Checklist 6** for tips on addressing cybersecurity in contracts.*
- Make sure to **consider risks related to artificial intelligence** - AI is making phishing and deepfake scams more sophisticated and convincing, and introduces new risks (such as ***data poisoning***, ***inference*** or ***extraction*** attacks). *See **Checklist 7** to learn more tips on **AI and cybersecurity**.*

This checklist is mainly based on the following resources and on insight from ACC members:

- ***Checklist: Ransomware Attacks - Prevention and Preparedness (US)*** by Jackson Lewis P.C.
- ***Cybersecurity Basics for In-house Counsel*** *ACC Docket*
- ***Tips for Responding to Cyber-Attacks and Insider Threats*** ACC Checklist
- ***Workplace Privacy, Data Management & Security Report Blog*** by Jackson Lewis P.C.
- ***Cybersecurity Awareness Audio Guide*** by Jackson Lewis P.C.

> If your organization's developers have not reached out to you yet, consider engaging in proactive outreach. It may increase the likelihood of counsel, and other security professionals, being brought in at the start of the product's development lifecycle, instead of at the end.
>
> **Robert Kang**
> *Professorial Lecturer,*
> The George Washington University Law School,
> and *former in-house legal executive.*

2. Ensure all relevant stakeholders fully participate and act on the results:

- Stakeholders who don't buy into this project **may restrict the flow of information which can lead to an inaccurate report**. They may also prevent the business from addressing major issues uncovered by the risk assessment.
- **The business must be ready to act upon the results**, or should at least document the reasons for not doing so. Companies that become aware of gaps but do not act upon them may face regulatory and litigation risks.
- **Include IT, Communications, HR, Marketing, Customer Relations**, and other relevant departments, depending on your business. Relevant stakeholders include individuals who have the power to make material decisions (such as turning off a service) or execute on such decisions.
- **Work with internal communications** to educate stakeholders on the importance of performing a risk assessment.
- It may also be helpful to **bring in your insurer or auditor** to help educate stakeholders.

3. Use attorney-client privilege, where applicable, to protect the risk assessment from being discoverable in litigation:

- This is particularly relevant in countries whose legal system allows for discovery in litigation proceedings.
- Deciding whether to administer a risk assessment under the attorney-client privilege and/or work-product doctrine requires **thoughtful deliberation**.
  - **In the US, courts distinguish** between assessments performed for legal risk purposes (for example, determining litigation exposure), versus those performed for business purposes (for example, determining the company's general ability to meet cyber threats).
  - **Performing these activities "under privilege" requires greater involvement by Legal.** Exercise great care when disseminating the results of those assessments for remediation purposes. These assessments often pinpoint areas for improvement, which organizations may not want to share with third parties, such as an adverse litigant.
- Consider having **outside cybersecurity counsel** conduct the assessment.
- **Segregate necessary regulatory disclosures** into separate deliverables from the rest of the assessment report.

4. Make the case for increased cybersecurity spending when needed:

- **Alternatively, if Legal is not the department driving the cyber budget,** gain familiarity with the relevant team's budget for cyber, and help them make the case for increased budget as needed.
- Data breaches **can cost millions of dollars**, even to small businesses.
- IT teams may not be as well-versed as Legal on the **business and legal justifications for increased cyber spending**.
- **Consider the full range of expenses**, including (but not limited to) employee training, awareness campaigns, and tabletop exercises.

5. Help define what the cybersecurity program looks like:

- Lead or participate in the risk management team to **decide the proper level of investment in cybersecurity**. This evaluation should also take into account privacy risks.
- Smaller organizations in the US may consider relying on ***guidance from the National Institute of Standards and Technology*** (NIST) of the US Department of Commerce, which sets out steps to protect controlled unclassified information.
- **Help decide when outside experts are needed,** including any retainers or stand-by support agreements with cybersecurity response specialists.

6. Balance business and security needs:

- **Ensure the C-suite is involved and informed as a key stakeholder.** Update them as necessary. Given the prevalence of cybersecurity risks, foster having the C-suite take a strategic leadership and oversight role in the organization's cybersecurity preparedness**.**
- **Get their feedback** to set an appropriate level of risk tolerance.
- **Provide the C-suite and other leaders with options.** Legal, business and technical stakeholders should work together to develop options. For example:
  - One option may be to immediately address all discovered gaps.
  - A second option may be to immediately address only high-risk gaps, and address other gaps over a longer period of time.

Encourage all staff to report to your IT security team anything strange or unusual that they may observe on any IT system – this can lead to discovery of an active threat.

Stephen H. Baird
Associate General Counsel
SITA

- **Promote security by design.**
  - Foster an approach where cybersecurity controls, vulnerability management, recovery, and other cybersecurity aspects are **included in the design of any service or product** the company is introducing.
  - **If your organization's developers have not reached out to you yet**, consider reaching out to them to discuss cybersecurity as a facet of the development process. It may increase the likelihood that legal counsel and security professionals will be brought in at the start of the products' development lifecycle, instead of at the end.
  - **Review security by design principles**, such as those communicated by government agencies, for example by the US ***Cybersecurity and Infrastructure Security Agency*** (CISA), the ***UK National Cyber Security Centre***, or the ***Australian Signals Directorate***.

7. Mitigate risks beyond the needs of legal compliance:

- Cybersecurity laws and regulations in specific states or countries sometimes aren't as strict as a **strong internal risk-mitigation strategy -** meaning that merely complying with law isn't always sufficient.
- On the other hand, **don't overlook compliance obligations** in developing your mitigation strategy.
- Your employees are **a vital line of defense** against cyber threats. **Implement training and awareness programs** to help employees recognize, prevent, and report cyber threats.
- Encourage all staff to **report to your IT security team anything strange or unusual** – this can lead to discovering an active threat.
- *See **Checklist 2** to learn more about **training employees on cybersecurity.***

8. Ensure that parties with access to your organization's data address cybersecurity:

- Incorporate and enforce data-security clauses in **contracts with third parties** that have access to your organization's sensitive data, such as IT and HR vendors, ***outside counsel***, and consultants.
- *See **Checklist 6** for **more tips on addressing cybersecurity in contracts**.*

9. Integrate cybersecurity into your legal operations:

- **Cybersecurity should be integrated in all parts of a company's operations**. That also includes how Legal itself operates.
- Ensure data security is integrated **into the legal department's own workflow tools and processes**.
- **For example**, this concerns Contract Lifecycle Management (CLM), matter management, document retention, and collaboration tools.

10. Keep track of evolving laws and regulations, as well as emerging threats:

- Increased cybersecurity reporting requirements may draw more **attention from regulators and shareholders** in the event of cyber incidents. For example, consider disclosure ***requirements*** from the US Securities & Exchange Commission (SEC), and the ***explanatory statements*** posted on the SEC's website.
- **Monitor changes** in the regulatory landscape. **Take into account the time it can take for the organization** to adapt and prepare for new regulations.
- **Educate the business** on evolving laws and regulations.

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	
Notes:	

CHECKLIST 2

A ROADMAP BY:

Joseph J. Lazzarotti
Jason C. Gavejian
Damon W. Silver and
Mary T. Costigan of
Jackson Lewis P.C.

With thanks also to ACC members for their insight.

Train Employees on Cybersecurity

Employee training is critical to your organization's cyber preparedness.

A vulnerable target and a line of defense:

- **Your employees are a critical line of defense** against cybersecurity threats, and a **potential vulnerability** in an organization's cybersecurity.
- **Human error is a cause or contributing factor in a majority of data breaches**, according to multiple ***studies***.
- **Bad actors often target employees** to infiltrate a company's systems, by using techniques such as phishing and social engineering.
- Your employees using your IT systems can be your "eyes and ears" to some extent, as **they can notice unusual activity** that can be the first indication of a compromise.

A key risk mitigation strategy is to train your employees regarding:

- Procedures for **handling data** and appropriate **methods for removing or securing** data during storage, use, or analysis;
- **Spotting** phishing attempts and social engineering attacks;
- What **type of data** is considered personally identifiable information; and
- **What to do** in the event of a potential cybersecurity incident.

There are numerous ways to design a training program to create awareness and build a culture of privacy and security in an organization. **The following are issues** organizations should consider when designing a training program.

1. Who will have responsibility for designing and implementing the program?

- If the company has a **privacy officer**, this might be a good choice, but it's not the only one. Otherwise, the **cybersecurity or IT team** might be suitable.
- There should be **an individual or department responsible** for maintaining the program.
- In-house counsel can help the privacy officer **leverage other internal resources**.
- For example, the training can be led or supported by the **Chief Information Security Officer** to ensure that training reflects the latest data loss prevention (DLP) tools the company has adopted and how to use them, as applicable.
- In-house counsel also can **work with the privacy officer** to ensure that "best practices" align with the organization's regulatory requirements and contractual obligations.

2. Who should be trained?

- In general, this should include **any workforce members with access to information the organization desires to safeguard -** this will often be the company's entire staff.
- **Employees as well as contractors, interns, volunteers,** and other **non-traditional categories** of workers should all be included. Appropriate contract clauses should also be imposed on vendors who will have access to the relevant information - *see **Checklist 6** to learn more tips on addressing cybersecurity in contracts*.
- **Even employees who are not permitted access to safeguarded data** may still have access to that information, inadvertently perhaps. They may need to be made aware of organizational protocols, such as **how to report a data security incident or breach**.

3. Who should conduct the training?

- Organizations may conduct training **in-house, outsource it, or a combination of both**.
- When training is performed in-house, the individual(s) selected to deliver the training **might depend on the information or safeguards being covered**. For example, if the safeguards at issue relate to information obtained by call center representatives, the call center manager might be a good choice to deliver the training.
- It is **not necessary, however, that a member of the IT, HR, or legal departments** deliver the training, or that it be a person with

technical IT knowledge. But the **ability to convey specific information** about organizational requirements, legal mandates, and use of technology to maximize security, will be helpful.

4. What should the training cover?

- The substance of the training will **depend on the organization, the data at issue, the audience,** and other factors.
- In general, training should **cover basics, such as what is confidential or personal information, or what is a data breach**.
- It also should communicate the organization's **policies and procedures**, not just general best practices.
- **Staff should be told:**
  - The IT security response team will never be upset if you report a suspicious IT irregularity to them which turns into a non-event. If something looks strange or unusual – for example, an unexplained email or sequence of data movements – it could indicate an active bad actor in the system.
  - It is better to be "safe than sorry" – **always report unusual observations**.
- **It also is helpful when training is role-based,** which can make the training more interesting for those being trained.
- Similarly, training programs can be significantly enhanced when they **use real situations that participants in the program can relate to** and apply in their positions within the organization. In general, the "basics" level training should cover the following topics:
  - **Introduction** to cybersecurity awareness.
  - **Recognizing** common threats.
  - **Safe internet/network** practices.
  - **Password** management.
  - **Email** security.
  - **Device**/physical security.
  - **Social engineering**/phishing awareness.
  - **Incident reporting** procedures.

> "Staff should be told: The IT security response team will never be upset if you report a suspicious IT irregularity to them which turns into a non-event."
>
> **Stephen H. Baird**
> *Associate General Counsel*
> SITA

5. When and how often?

- Basic privacy and security training should be provided **before an individual obtains access** to confidential or personal information.
- At a minimum, the basic cybersecurity principles should be conveyed **at least annually** thereafter. **More frequent training** may be required for teams that handle high risk data such as social security, financial, or health information.
- Training may also be needed **after significant changes in policies**; **following increases in levels of access or sensitivity** of information; to react to **changes in technology**; in light of **new threats or security measures**; and **following a security incident** and other situations, such as a merger or acquisition.

6. How should training be delivered?

- There are **many ways to deliver a consistent message** about data security throughout an organization.
- **Consider** policies, notices, newsletters, intranet dashboards, in-person sessions, online courses, videos, testing, tabletop exercises, employee resource groups, or a combination of these options.
- **The ability for participants to interact and ask questions** can be critically important for them to understand their responsibilities as they relate to the business.
- **Consider conducting phishing simulations** that expose employees to realistic simulated phishing attempts. These simulations can offer **metrics** regarding your workforce's readiness to spot and report suspicious communications. There are vendors who provide this type of employee training service.

7. Should training be documented?

- **Yes.** In some cases, documentation is required by regulation (such as under the US ***Health Insurance Portability and Accountability Act*** (HIPAA)). However, an organization will be in a much better position to defend its data privacy and security practices if it **can show that it maintains a comprehensive training program.**
- This generally means that the organization **tracks the materials covered** in the training **and those who attended** or received the information.
- **Cyber insurance providers** typically require documented training.
- Also, when evaluating an organization's cyber-readiness, **judges and international arbitrators** like to see evidence of training.

TAKE ACTION: Write one or two steps that you plan to implement.	
Describe	By what date?
1.	
2.	
Notes:	

Learn more

- ***Developing a Privacy and Cybersecurity Training Program for Employees*** by Jackson Lewis P.C.
- ***Cybersecurity Awareness Month Series: Employee Cybersecurity Awareness Training*** by Jackson Lewis P.C.

CHECKLIST 3

Prepare for Data Breaches

It's essential for your organization to have a plan for responding to a potential data breach in a timely and efficient manner. Below are preparedness strategies.

Quick Tips

- **A data breach can take many forms.** For example, it can include a **lost device** containing sensitive data, the **theft of paper files** containing personally identifiable information, **electronic data stolen** by an employee, a **misdirected email** containing unsecured sensitive data, a **ransomware attack**, a **hacking** incident, or a **business email compromise**.
- **An Incident Response Plan (IRP) should be high-level, scalable, and adaptable**, since no two data incidents are alike.
- **A good IRP should serve as a road map** for responding to an incident.
- **A good IRP should also be succinct.** Team members will not have the time or focus to read and digest a voluminous document in the midst of a data incident.
- **A good IRP should be practiced.** Tabletop exercises are an excellent way to practice your plan. Conduct tabletop exercises with the relevant stakeholders (including the business).

1. Develop an *incident response plan* and a *breach notification policy* prior to any attack:

- Plan **a cross-disciplinary team** to respond to data breaches. Remember that cybersecurity requires a whole-of-company approach to implement. The IT team is typically a necessary stakeholder, but by itself is not sufficient. *See Section 2 for more on forming such teams.*
- It may start with a **template incident response plan**. However, **using a mere template plan may leave out critical regulatory requirements** and issues specific to an organization that should be addressed. An IRP that doesn't align with how you do business makes it less valuable and may become a liability during litigation.
  - For example, in the United States, **various data breach notification requirements** have emerged across jurisdictions, regulatory agencies, and industries.

WITH THANKS TO:

Joseph J. Lazzarotti
Jason C. Gavejian
Damon W. Silver and
Mary T. Costigan of
Jackson Lewis P.C.

and the ACC members who contributed to this checklist.

> **Flow charts and diagrams** are handy to use in case of an emergency. They help teams quickly understand their duties and responsibilities.
>
> **Bunny Smith**
> *Global Cybersecurity Counsel*
> Yahoo!

- For organizations subject to the European Union (EU) General Data Protection Regulation, consider whether the incident **will trigger breach notification requirements across multiple EU member states** and identify which Data Protection Authority should be notified.
- Similarly, for organizations subject to Canada's data protection laws, consider whether the incident will trigger reporting obligations under multiple provincial or territorial laws.
- Consider all applicable privacy and cybersecurity laws and data breach notification obligations in all relevant countries (which may be stricter than US laws, for example in terms of notification obligations and timelines). **Identify** notification obligations under **state and international data breach law** - i.e., which state, jurisdiction, or district laws would apply?
- Consider the **varying contractual obligations your organization may have to customers** through multiple and often conflicting services agreements.
- Consider the **subsidiaries and affiliates** your plan may need to address.
- Your incident response plan needs to **prepare the incident response team to identify these variations** to help direct its response.
- **Develop playbooks for incident scenarios** that your organization may face - such as, without limitation, a business email compromise, or a Distributed Denial of Service attack (DDoS).

- **Be prepared to move quickly** through the response process to minimize disruption to operations, economic loss, and reputational harm. Delay in identifying and responding to an incident can invite regulatory scrutiny.
- **Understand the terms of your cyber insurance policy,** including how to activate it, required authorizations, retention, and coverage (e.g., forensic investigation, legal fees, ransom payments, credit monitoring services).
  - Your policy may have **preferred vendors** for remediation efforts. Knowing who to call in an emergency rather than scrambling can save time and money.
  - *See more tips on cyber insurance in* ***Checklist 4.***
- Determine whether your IT department or managed service provider has the **experience, qualifications, and equipment** to handle incident containment, a forensic investigation, and remediation - in many organizations, this will require external specialist support.

- **In-house counsel can play an important role** here to help minimize legal risk caused by well-meaning senior leadership who may not be best positioned to carry out certain necessary steps in a data incident investigation.

- **Identify potential reporting obligations,** such as (without limitation):
  - in the US, as required by federal regulators, state attorneys general or other state agencies, tax authorities, insurance commissioners, the Department of Health and Human Services (HHS), the Securities and Exchange Commission (SEC), or the Cybersecurity and Infrastructure Security Agency (CISA),
  - to the relevant EU member state's ***Data Protection Authority*** (DPA) or the "lead" DPA for cross-border processing,
  - to the UK Information Commissioner's Office where the breach could likely result in a risk to people's rights and freedoms,
  - to the ***Australian Information Commissioner*** after becoming aware of any reasonable grounds to believe there has been an eligible data breach,
  - to Brazil's Data Protection Authority, the ***Autoridade Nacional de Proteção de Dados*** (ANPD), and
  - to India's ***Computer Emergency Response Team*** (CERT-In).
- **Develop a strategy for notifying regulators** where multiple jurisdictions are involved – for example, whether to first notify the regulator with the shortest timeline, or whether to notify all regulators at the same time after gathering adequate information.
- **Identify contractual obligations** to notify business partners, clients/customers, covered entities, and other parties.
- **Keep in mind that** whether the organization is providing notice to a regulator or affected individuals, **reporting obligations timeframes can vary significantly** depending on the applicable law or regulation.
- Here again, **in-house counsel's knowledge of the organization can play an important role** in planning for and implementing the compliance requirements that may apply to the organization depending on its organizational structure, industry, business locations, contractual and ethical obligations, etc.
- **For example, if the organization is publicly traded in the US**, it will quickly need to **assess "materiality"** under SEC regulations and ***satisfy applicable reporting obligations***, which may include ***filing Form 8-K within four days*** of that ***materiality determination***.

- **If the organization is subject to the EU GDPR (General Data Protection Regulation) or the UK's *Data Protection Act*,** it will need to quickly assess whether the breach could likely result in a risk to people's rights and freedom and, as needed, provide notice to the appropriate regulator within 72 hours.
- **Under Australian law,** organizations must notify the ***Australian Information Commissioner*** (AIC) and affected individuals "as soon as practicable" after becoming aware of any reasonable grounds to believe there has been an eligible data breach.
- **Organizations subject to Canada's PIPEDA** (***Personal Information Protection and Electronic Documents Act***) must quickly assess whether the breach creates a real risk of significant harm and, if so, notify any government institutions or organizations that it believes can reduce the risk of harm that could result from the breach or mitigate the harm.
- **Brazilian *law*** requires data controllers to notify affected individuals and the Data Protection Authority (ANPD) within ***three working days*** after becoming aware of an event related to a personal data beach.
- **Under India's laws**, keep in mind that organizations are required to report certain cyber incidents to the Indian ***Computer Emergency Response Team*** (CERT-In) ***within six hours of becoming aware of the incident***. **In addition,** once the Digital Personal Protection Act of 2023 comes into effect, in the event of a personal data breach, data fiduciaries and data processors would need to inform affected individuals (data principals) and the new Data Protection Board of India.
- Consider which state or global regulators must be notified **before notifying any affected individuals** (e.g., under New Jersey law) and/or whether the organization is required to provide a preliminary description of the incident within days of the incident (e.g., under Vermont law).
- Work with appropriate stakeholders to **review and update the organization's information security program**.
  - In the event of a reportable data breach, regulators may require confirmation that the organization has a **written information security program (WISP)** or **appropriate administrative, physical, and technical safeguards** in place (e.g., Massachusetts, U.S. Department of Health and Human Services Office for Civil Rights (HHS OCR), UK Information Commissioner's Office).
  - In addition, regulators may request evidence that the organization has **conducted employee security awareness training**.

- Include in your plan to **remind involved parties to preserve evidence of the incident** (e.g., creating system images, etc.) as they remediate the incident.
  - This evidence **may be critical for determining** whether the event is a security incident or a reportable data breach.
  - It may also be **valuable for any law enforcement investigation**.
  - In addition, at some point, **potential threats of litigation or investigation may require a litigation hold** to be implemented.
  - Legal should direct this process and **ensure privilege is maintained.**
  - Global data privacy laws generally impose an **obligation of accountability** on organizations. Accountability would typically include having a robust cybersecurity program, but also training and awareness programs to ensure that employees and other stakeholders are aware of relevant laws and obligations.

2. Put together the responsible teams, both internal and external:

- Having a broad perspective of the entire business and operations, in-house counsel must **play a valuable role in ensuring that key internal stakeholders are part of the team**.
- **Depending on your organization**, the internal team may include leadership and the C-suite, IT, Legal, Finance, Operations, Communications, Human Resources, Customer Relations, and others. During the course of responding to an incident, most or all of these areas will likely need to be tapped for information or their expertise about how systems or the business operate.
- Team members should include **only internal individuals with a "need-to-know"** in an effort to protect any privilege and minimize the risk of leaks.
  - Designate individual(s) **who will have final decision-making authority**. This will help avoid delays caused by having too many participants.
  - **External resources** may include outside counsel, forensic investigators, incident response firms, insurance carriers, data mining vendors, ransomware negotiators, printing and mailing vendors, and public relations. To avoid delays, such vendors should be under **retainer agreements** and should be **approved by the organization's insurance carrier in advance.**
  - **Ensure that each part of the team understands** the larger data breach plan and their role in it, including methods for protecting any privilege.

> Consider creating a triage log so that all hunts, shutdowns, remediations, and actions are captured in a spreadsheet. This will help the team know what steps have been taken by everyone. It may also spark ideas as to what steps must come next.
>
> **Bunny Smith**
> *Global Cybersecurity Counsel*
> Yahoo!

- **Consider having the plan require external counsel to be engaged** as soon as possible to protect the investigation and incident response under the attorney-client privilege (e.g., engaging a forensic investigation firm on behalf of the organization, and reviewing external communications). Appropriately structured in-house counsel teams can also be used to protect privilege, but there are benefits to using outside counsel.
- **Be aware of entrenched relationships** that the IT and communications departments may have with external vendors.
  - Leveraging those existing external relationships **could jeopardize privilege** because the relationships predated the incident and were not initiated through legal counsel for the purpose of assisting it to provide legal advice.
  - If such entrenched relationships exist, in-house counsel and their internal clients should proactively discuss the upsides and downsides of **building out independent relationships between counsel and those vendors** for incident response.
- Additionally, the organization should **carefully consider its communications with insurance brokers and carriers,** to help maintain privilege where possible.
- **Include confidentiality and data protection provisions** in any services agreement with third parties assisting in the incident response.

3. Take advantage of available government resources:

- In-house counsel can work with the organization's compliance team to **identify its primary regulatory oversight agencies**, which would be sensible starting points for places to leverage government resources.
- For example, in the US, **health systems** would likely look to the ***HHS Office for Civil Rights***, **educational institutions** would look to the ***US Department of Education***, and **credit unions** should examine recent data breach regulations issued by the ***National Credit Union Administration***.
- **Many other governmental entities, however, have been developing helpful resources** to address various security risks and incidents, and responding to them.
  - Such entities include the US ***Cybersecurity Infrastructure Security Agency***, ***Data Beach Resources*** of the Federal Trade Commission, the ***Federal Bureau of Investigation***, the Canadian Centre for Cyber Security's resources on ***Developing your incident response plan (ITSAP.40.003)***, and the UK ***National Cyber Security Centre***. They have resources to help in developing a cybersecurity plan, as well as to help respond

to attacks. US state attorneys general also have available information and resources related to data breaches.

- The European Data Protection Bureau's ***Guidelines 9/2022 on Personal Data Breach Notification Under GDPR*** includes an array of information on identifying a personal data breach, providing information to the supervisory authority, and handling cross-border breaches occurring outside the EU.
- The Office of the Privacy Commissioner of Canada provides ***data breach reporting guidance*** for organizations subject to Canada's PIPEDA.
- If your organization is covered by the Australian Privacy Act 1988, information on responding to a data breach is available at the ***Office of the Australian Information Commissioner.***

4. Your Incident Response Plan should account for emerging *artificial intelligence threats*:

- **AI-powered security tools can help** guard against emerging threats, such as deepfakes and ransomware. AI can better detect AI-based threats and, when authorized, can deploy patches fast enough to counter them.
- However, these should not be the only tools used to detect or prevent threats.
- Conduct **regular risk assessments** and **update your plan** to address new findings.
- Review and update your plan **after any significant change to your environment,** for example, an increase in remote workforce, addition of personal devices ("BYO"/Bring Your Own devices), expanding the business to new locations, working with new customers, or service providers requiring access to systems.
- **Monitor available resources** for information about **emerging threats**. For example, the US FBI's ***official alerts and statements***, US CISA's ***cybersecurity alerts and advisories***, the ***Center for Internet Security's advisories,*** the ***Canadian Center for Cyber Security***, the ***European Union Agency for Cybersecurity*** (ENISA), and the ***Australian Signals Directorate***. Organizations that are members of Information Sharing & Analysis Centers/Organizations (***ISACs/ISAOs***) may also receive information from those sources.

5. Prepare for organizational continuity in the event of an attack:

- Certain attacks such as ransomware **can cause severe disruption**. Design your plan to help navigate those effects as efficiently as possible.

- **Identify** which systems and data are **critical to daily operations**.
- **Include safety measures** like backup files, system safeguards, and replacement equipment to keep your organization going during and after an attack.
- **Perform backups** on a regular basis and **segregate backup storage** devices and files from the system to minimize the risk of compromise in an incident.
- **Review available resources for guidance**. For example, CISA's resources on:
  - ***Business Continuity in a Box***
  - ***The Continuity of Operations: What You Need To Know***
- **Consider how to respond to ransomware:**
  - The **official position of many government agencies** is not to pay ransom.
  - A couple of US states have passed **laws prohibiting payment** in certain cases (***North Carolina*** and ***Florida***).
  - Member nations of the ***International Counter Ransomware Initiative*** (CRI) have pledged to no longer pay ransom demands.
  - However, **some organizations may consider that in some limited cases, making a ransom payment** may be justified, for example as a last resort business critical continuity response.
  - **In-house counsel can play an important role** in helping to guide the process of making that decision, with **some of the steps being included in the incident response plan**.
  - Before any ransomware incident takes place, **define a ransomware response strategy**, which includes the process for determining whether and how to make a payment. Keep in mind applicable regulations and the need to conduct sanctions checks before payment.
  - **Consider who should be involved in the process**, what third party to partner with on negotiations and facilitating payment, as well as compliance issues. These are important considerations to be examined before an incident occurs.
  - From a compliance perspective, it is important that the organization **take steps to avoid making a payment in violation** of applicable laws or regulatory agencies' rules or guidance (such as the guidance from the Office of Financial Asset Control (OFAC) in the US). Learn from the ***guidance issued by the US Department of the Treasury***.

- **Consider the reputational implications** of making a ransomware payment.
- **Also consider how exactly a ransom will be paid,** especially if the attacker requires to be paid in the form of cryptocurrency – consider whether your organization has a vendor that can assist with this, or whether your company's bank would help you with such payment process.

6. Include law enforcement in your response and plan to *notify* authorities:

- **The decision to notify law enforcement** of an incident and/or respond to their requests for information will depend on **many factors**, such as, without limitation:
  - The type of industry,
  - The size and scope of the incident,
  - Details concerning the attacker,
  - The actual or potential knock-on effects on other parties, as well as
  - Whether such notice is legally required,
  - Whether you intend to rely on an exception (e.g., a "risk of harm trigger") that is only available following consultation with law enforcement, and
  - Whether law enforcement assistance is needed to mitigate harm (e.g., to recover misdirected wire payments).
- In-house counsel can play an important role here. **Requirements to notify law enforcement** at different stages of the incident response process are expanding. But even apart from legal requirements, it is a good business and legal practice to **cultivate relationships with law enforcement.**
- **Consider connecting with primary regulators ahead of a data incident**. Having an established relationship can help to facilitate notice and get support if needed when facing an attack. Law enforcement personnel can be tremendously helpful.
- **Prepare to notify law enforcement** (e.g., state and/or federal) and government agencies, as appropriate. For example:
  - The FBI through the *IC3 portal* and CISA through *Report to CISA*.
  - *The Australian Signal Directorate through an online report.*
  - *Online to the Canadian Center for Cyber Security*.
  - The *Europol* website includes links to reporting websites for EU member states.

This checklist is based mainly on input from Jackson Lewis P.C., as well as insight from ACC members and the following resources:

- ***Data breach checklist*** by ACC
- ***Ten Key Items to Strengthen Preparedness for Data Incident Response*** by Jackson Lewis P.C.
- ***Data Breach! A Playbook for The First 72 Hours*** by Stephen H. Baird and Simon Elliott
- ***Tips for Responding to Cyber-Attacks and Insider Threats*** by ACC
- ***Data Incidents and Response*** by Jackson Lewis P.C.
- ***Data Breach Checklist (US)*** by Seyfarth Shaw

7. Test your response plan before an incident happens:

- Periodically **run tabletop exercises** that cover different types of incidents, including the decision-makers in your organization.
- Remember tabletop exercises can be held **at any level of the organization**. For example, it may make sense to have an exercise just for IT, executives, or board members.
  - Some tabletop exercises are **strategic** and intended to allow management and/or the board to think, for example, about the situations in which they might consider paying a ransom.
  - Other tabletop exercises are **more operational ones** intended for employees to practice preparing and releasing communications, restoring a back-up of systems and data, etc.
- A tabletop exercise **often takes 2-3 hours**. It will provide your internal response team with **an opportunity to practice** their roles, identify potential issues, and discuss best practices.
- **The exercise should include** (in a controlled environment) identifying an incident, initiating the IRP, containing the incident, remediating and restoring operations, and performing internal and external communications while maintaining legal privilege.
- **Consider including some of your external partners in this process**. At a minimum, it could allow all members of the anticipated team to begin working together, become familiar with the respective organizations, and better position the organization for a more seamless response.

8. Review and update your plan regularly:

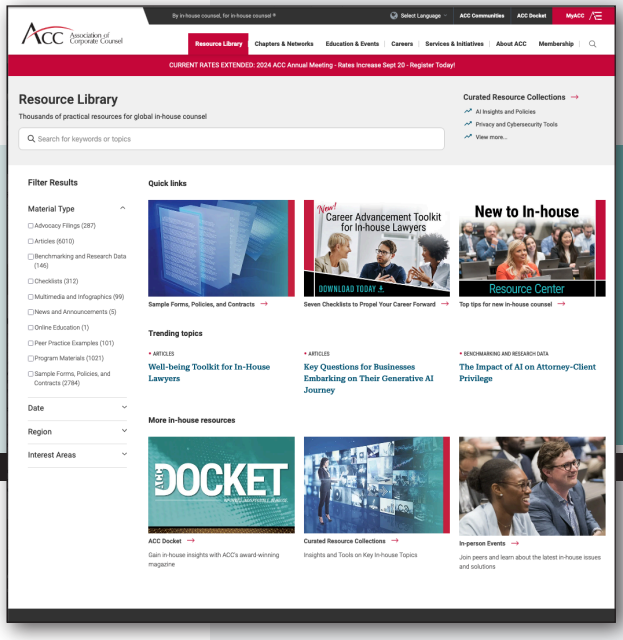
- **After you run tabletop exercises**, update your plan to address lessons learned.
- **Notify all team members about updates** to the plan and how their **responsibilities may have changed**.

TAKE ACTION: Write one or two steps that you plan to implement.	
Describe	By what date?
1.	
2.	
Notes:	

Visit the

ACC Resource Library

Find articles, checklists, sample contracts & policies, and more resources for in-house lawyers.



CHECKLIST 4

A CHECKLIST CONTRIBUTED BY:

Joseph J. Lazzarotti
Jason C. Gavejian
Damon W. Silver and
Mary T. Costigan of
Jackson Lewis P.C.

With thanks also to ACC members for their insight.

Cybersecurity Insurance Tips

Data breaches can lead to significant costs. Insurance plays an important role in protecting against cybersecurity risks. The following are key points to consider when evaluating coverage options and purchasing your policy.

A few facts:

- The global **average cost of a data breach in 2024** was $4.88 million (USD), according to IBM's *Cost of Data Breach Report*.
- A *2024 Sophos survey report found* that organizations that paid a ransom reported paying an average of $2 million in 2024 (compared to $400,000 in 2023), and that the average recovery cost excluding ransom was **$2.73 million (USD).**
- In the US, the FBI's Internet Crime Complaint Center (IC3) *reported* **2,825 complaints of ransomware in 2023**, costing $59.6 million (USD) in adjusted losses.
- **Ransomware** *will cost organizations $265 billion (USD)* by 2031, according to Cybersecurity Ventures.

1. Identify the potential triggering events and the types of losses for which you may need coverage:

- **Identify the potential triggering events** – situations under which you would want to file a file an insurance claim. For example, consider situations where a ransomware attack occurs on a vendor's sub-processor or subcontractor; phishing attempts or social engineering attacks on your employees; negligence by your employees, etc. – does your existing or potential insurance policy cover the types of triggering events that you have identified?
- **Lost revenue due to business interruption.**
  - This is most notable in the case of **ransomware attacks**, which can cripple business operations for hours, days, or even weeks.
  - Consider **what this means for your business in your industry,** for example:
    - **delays** in the ability to treat patients or accurately update medical records and billing systems,
    - **pulling down a website** through which customers purchase most of your products,

    - **inoperable control systems** stalling progress on the factory floor, and
    - **impeding the ability** of professional service providers to **access work product** needed to serve customers (e.g., lawyers in the middle of trial).
- **Making ransom payments** to bad actors to recover your data or suppress its disclosure on the dark web (again, in the case of ransomware incidents).
- **Investigating the nature and scope of the incident**, whether resulting from ransomware, business email compromise, employee error or misconduct, etc., and **taking action to secure your systems**.
    - This often requires the retention of third-party legal and digital forensic incident response **experts**.
    - Beyond system security and forensics, costs also could include **efforts to determine what personal data or other information has been impacted**.
    - In many cases, **data mining and document review** services may be necessary, particularly for large data sets.
    - These costs can be significant and unpredictable.
- **Restoring data and information systems**, most notably in ransomware attacks. This may include replacement of systems and equipment, but also salvaging backups to ensure systems and applications are safe and efficient to operate.
- **Misdirected wire transfers** that you made to the bad actor or that your vendor made when attempting to pay you.
- **Vendor breaches** impacting your data, your customer's data, or your ability to do business.
- **Analyzing your legal notification and reporting obligations**, and developing your associated **legal and public relations** (PR) strategy, often with guidance from outside counsel and, in some instances, PR experts.
- **Providing communications, notifications, and submitting government reports.**
    - This can be a significant and costly process**, particularly when the notification population is large**.
    - It may involve **regular communications to customers** about the status of your systems and **providing instructions to reconnect** with your service.
    - It may involve **evaluating many service agreements with customers** to understand your notification obligations.

- **Providing identity theft protection services,** which are sometimes legally required.
  - As of July 30, 2024, **six jurisdictions in the United States require ID theft and/or credit monitoring services** to be provided for certain data breaches – ***California***, ***Connecticut***, ***Delaware***, ***Massachusetts***, Pennsylvania, and ***Washington D.C.***
  - Requirements to provide free ID theft and/or credit monitoring services are relatively unique to the U.S. However, **most jurisdictions with data breach notification laws require taking steps to reduce the risk of harm** that could result from the breach. Providing these services, to the extent they are available in the jurisdiction, could be viewed as such a measure.
  - **Some policies may only cover** this cost when such services are **legally required**.
  - **For breaches affecting individuals across many states**, you may want to provide these services **more uniformly**.
- **Operating a call center to field inquiries** from notice recipients - which, again, can be costly if the notification population is large.
- **Responding to government investigations** and **paying fines or administrative penalties** imposed by a regulator or a governmental authority (if any).
- **Defending against government investigations and litigation**, including class actions, and paying damages and settlements (if any).
  - Litigation may arise not only in cases where your organization has experienced a breach. You can also be pulled into a litigation where a **vendor handling your data has been breached**, resulting in the exfiltration of personal data.
  - Separately, **a vendor breach that impacts your operations** also may lead to litigation, such as in cases where your organization is unable to process payroll or some other critical function, triggering **claims from affected persons or the state.**

2. Evaluate the amount of coverage needed. Consider these points:

- The **scope of the organization** that would be covered under the policy, including **subsidiaries, affiliates, and divisions**.
- Do you handle more **sensitive personal information** like protected health information, payment card information, social security numbers, driver's license numbers, biometric information, or genetic information?

- Because these types of information are more heavily regulated and are considered more "valuable" to data subjects, the degree to which you handle them impacts the probability that you will experience a reportable breach, as well as the likelihood that such breach will result in government investigations and/or litigation.

- **Your regulatory environment.** For example:
  - What is your **regulatory and enforcement landscape** in the jurisdictions in which your business operates?
  - Is your business in **critical infrastructure, health care, financial services, or retail**? Businesses in these sectors may be subject to robust industry-specific data privacy and security requirements and, accordingly, may have increased exposure to data privacy and security risk.
  - Is the organization **publicly traded**? US SEC regulations impose heightened data security obligations on publicly traded organizations.
  - **Do you handle personal information related to large volumes of consumers** or are you a B2B business that only maintains such data for a few hundred employees and their family members? Organizations that handle large volumes of personal information have greater exposure to breach-related costs (e.g., investigation, response, notification, credit monitoring, etc.) than those that handle modest amounts of such information.

- The **strength of your policies, procedures, practices, and controls** concerning critical information systems, along with your organization's level of preparedness to respond to an incident.
  - Organizations that have higher levels of confidence in their data security programs may feel comfortable purchasing policies with higher deductibles and/or lower limits in return for lower premiums.

- **Contractual and other obligations to customers and other organizations** pertaining to the **data your organization handles or services it provides** on behalf of customers and others.
  - If you provide services to customers in highly-regulated industries, and therefore will be processing data subject to rigorous data privacy or security frameworks, you will likely be required to assume significant data privacy and security obligations by contract. You will need to ensure you are appropriately insured against the associated risk.

- How much of your **sensitive / heavily regulated data is maintained by third parties,** and how strong are **your controls** for vetting and monitoring those third parties' data security postures?
  - As with evaluating the strength of your own data security safeguards, you will need to evaluate those of the third parties that have access to your data.

This checklist is mainly based on input from Jackson Lewis P.C., as well as on the following resources, and on insight from ACC members:

- ***What to Look for in a Cyber Insurance Policy***, a podcast by Jackson Lewis P.C.
- ***Does Your Cyber Insurance Policy Look More Like Health Insurance?*** by Jackson Lewis P.C.
- ***Data breach checklist*** ACC Checklist

  - If those parties experience breaches impacting your data, you may be financially responsible for the resulting costs and need to insure yourself appropriately.
- How often do your employees make wire transfers and in what amounts? And how strong are **your controls to prevent misdirected wires**?
  - Misdirected wire transfers can be a major source of liability resulting from cyberattacks – e.g., your employee may unknowingly send a wire payment to a bad actor rather than your vendor, and then remain on the hook to satisfy the vendor's invoice.
  - If your organization **regularly makes wire transfers**, or transfers **large amounts** (even if infrequently), that should be a factor in selecting insurance coverage.
- **If you lost access to key systems and data**, how much would that cost you per day?
- Based on publicly available information about your business's financials, **how large of a ransom payment might a bad actor seek to extract** from you in return for providing you with a key to decrypt your data, or to refrain from leaking your business' data on the dark web?
- **Do you have other insurance coverage**—besides cyber—and/or internal reserves to defray the costs associated with investigating and responding to a data breach?

3. Evaluate definitions, potential exclusions, and sub-limits:

- Confirm that your organization's **application for coverage** and other **representations during the underwriting process** will not compromise a claim due to **inaccurate or incomplete statements**.
  - In-house counsel may want to **play a more active role with IT and risk management concerning these representations**.
  - These representations can later become **important factors in coverage determinations**.
- **If your policy or policies include sub-limits**, do those limits **align with expected costs** in the following areas:
  - Outside legal counsel
  - Digital forensic incident response
  - Ransom payments
  - Misdirected wire payments
  - Data restoration
  - System restoration

  - Business interruption
  - Notification
  - Offering identity theft restoration services
  - Responding to regulatory investigations
  - Defending against litigation
- Are any of the above areas **excluded from coverage?**
- **Consider whether a "war exclusion" applies.** Depending on the country from which the cyber-attack originates, this could negate the policy.
- **What steps are required on your end to maintain coverage** and **are you able to take those steps** – e.g., utilizing Multi-Factor Authentication (MFA) across key applications, maintaining air-gapped backups, vetting and contracting with vendors?
- **Ensure the organization is aware of the need to timely report** incidents under the policy.
- **Review how key terms are defined** within the policy, such as "cybersecurity," "incident," "privacy," and "breach." Also be aware of how these definitions may change at renewal.
- **Cyber insurance is typically on an annual renewal**. Request your insurer (or broker) to provide a list of policy changes with written explanations of what the changes mean.

4. Pre-clear outside experts:

- In the event of an incident, you want to **be prepared to move fast**.
- **Consider getting advanced approval from your cyber insurance carrier** to use your preferred outside experts—in particular, your legal and digital forensic incident response experts. This helps you hit the ground running if an incident occurs.
- **Schedule exploratory meetings** with some of the outside experts on the carrier's panel.
- **Make selections in key areas** and consider taking some preparatory steps to build familiarity, such as through **joint tabletop exercises**.
- **Get contract negotiation and other housekeeping issues out of the way** for the established team – have these signed and in place, and update annually. Consider putting in place **master services agreements with the key vendors** that are on panel with your organization's carrier (such as legal, forensics, breach notice, and other vendors).

5. Evaluate the "insurance experience" you can expect:

- What is the **claims team** like and **what resources does the carrier make available** to help address data risk.
- **Claims processing can be challenging** on many levels.
- While policy limits and exclusions are important, you also want to **assess the level of support from the claims team** you can expect from the carrier at such a critical point for the business.
- Carriers generally **have assembled resources for their insureds** to help them **minimize the likelihood and/or impact of a data breach**.
  - When considering a carrier, **review these options** and use them once coverage is bound.
  - **Their panel providers often also provide products and services**, sometimes at no cost or at significantly reduced cost, to assist the insured's preparedness.
  - **Consider how the insurance carrier has acted in the past, regarding previous claims.** What are the situations in which they have rejected a claim on a relevant policy?

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	
Notes:	

Responding to Cyber Incidents

Help the company navigate the crisis. Rapid coordinated response is key. The following represents common "stages" of the incident response lifecycle. Note that the steps are not strictly linear. Actions taken in one stage may overlap with actions taken in another stage.

1. Triage, mobilize the team, apply first aid, implement the response plan, and document your response:

- **Promptly** mobilize the "first responders" team – often involving members of IT, Legal, Communications, and other teams.
- **If an incident response is intended to be under legal privilege**, have Legal designated as the incident commander and provide direction to the other teams.
- **Ensure "first aid" measures are taken** to contain and investigate the issue, assess its severity and scope, stop ongoing threats, and patch existing holes in your cybersecurity.
- **Ensure the decision-making is clearly allocated** per the response plan.
- Consider what **internal and external-facing systems**, services, and workflows are impacted, and **what data** may have been compromised – or is possibly being actively compromised if the incident is discovered while ongoing.
- **Determine temporary measures** needed to ensure business continuity, which may involve degraded service.
- **Document the team's actions** - meetings, attendees, decisions, measures taken. If decisions deviate from the plan or policies, document the reasons why. Organizations should **keep robust internal documentation** of incidents and of their notification analysis – not only is this good practice, there are also legal requirements (such as, without limitation, from the EU's GDPR, the US SEC, etc.).

2. Investigate and engage help as needed:

- **Engage** outside counsel to advise on regulatory obligations and notification requirements, if any, and potentially to engage forensic services firm(s).
- **Engage** technical experts as needed to investigate and stop the threat.
- **Engage communication experts** as needed to help with public-facing and staff-facing communications.

CHECKLIST 5

This checklist is mainly based on the following resources and on insight from ACC members:

- ***Data Breach! A Playbook for the First 72 Hours*** by Stephen H. Baird and Simon Elliott
- ***Data Breach Notification Chart (US)*** by Jackson Lewis P.C.
- ***Sample Notice of Data Breach Letter (US)*** by Jackson Lewis P.C.
- ***Data Breach Checklist – 12 Steps for the First Hours*** an ACC Checklist
- ***Cyber Incident & Data Breach Management Workflow*** by Exterro
- ***The Exterro Quick Guide to Data Breach Response*** by Exterro
- ***Tips for Responding to Cyber-Attacks and Insider Threats*** an ACC Checklist
- ***Putting a Data Breach to Bed: A Checklist of What Counsel Needs to Do After a Breach Response*** by Anand Raj Shah, Drinker Biddle & Reath

- **Ask the hard questions** to understand the scope of the issue, however unpleasant the situation may be for business stakeholders to hear about.

3. Communicate deliberately and as needed:

- **Don't guess or make speculative or hasty statements**. Stick to known facts. Keep in mind the known set of facts is likely to evolve rapidly as new findings appear.
- **Communicate with senior management and the board** – keep them informed, share estimated remediation costs (knowing that precise estimates are likely impossible in the early days/weeks), explain options and your recommendations, and seek their guidance as needed. Update them regularly regarding evolutions.
- **Consider the need to communicate** with staff, regulators, clients, and the public.
- **Ensure communications are vetted** and made by the designated channels, and that requests for comments are promptly redirected to the designated person.
- **Journalists may give you little time** to offer comments before they publish a story. Ensure press requests are directed to the designated spokesperson.
- **Keep employees adequately informed and updated** at appropriate junctures of the situation.
  - Keep in mind they may be hearing news reports about the situation and may be speculating.
  - Consider providing employees with a certain level of detail.
  - Consider providing them with a script or template response in case they are approached by an external party or by the press.

4. Comply with notification requirements:

- **Time is of the essence** given regulatory and contractual requirements.
- **Keep in mind** notification to data subjects and/or authorities may be required even for suspected breaches.
- If you don't have the internal resources, **engage outside counsel early** to help you understand and comply with these requirements.
- Don't forget to notify your **company's insurance carrier** promptly as required by the cyber insurance or other policy.

ALSO CHECK OUT:

Multi-factor Authentication (MFA) Bypassed to Permit Data Breach
by Joseph J. Lazzarotti, Jackson Lewis P.C.

The Broadening Data Security Mandate: SEC Incident Response Plan and Data Breach Notification Requirements
by Damon W. Silver and Melissa Pascualini, Jackson Lewis P.C.

HIPAA Security Incident Assessment Tool
by Jackson Lewis P.C.

5. Assess the damage, remediate, review, and improve:

- As your team identifies vulnerabilities or failures in your cyber defenses, ensure those get **patched promptly** to prevent new similar incidents.
- Support efforts to **restore service levels**.
- Consider the need to extend **credit monitoring services** to data subjects.
- **Conduct an after-action review** once the crisis is resolved: Assess how effective the response was, what worked well, and what to do differently. Share lessons learned, and improve your policies and cyber and crisis response plans.

> "You should aim for communicating the clearest picture possible, in a way that can be substantiated later."
>
> **Stephen H. Baird and Simon Elliott**

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	
Notes:	

CHECKLIST 6

Addressing Cybersecurity in Contracts

Third parties with which your organization does business may be a source of cyber-vulnerability. Mitigating that risk is important.

WITH THANKS TO:

Joseph J. Lazzarotti
Jason C. Gavejian
Damon W. Silver and
Mary T. Costigan of
Jackson Lewis P.C.

and the ACC members who contributed to this checklist.

1. Consider inserting clauses that require certain minimum levels of security:

- Before entering into a contract, perform adequate **due diligence** on the third parties that you plan to deal with.
- Consider the **level of detail and timelines** you'd like to specify in the agreement.
- Consider mentioning the adoption of appropriate **technical and organizational measures.**
- For contracts that involve particularly **sensitive data or personal information**, consider adding a **data protection addendum** to the main agreement.
- If **cross-border transfers** of personal data are involved, **consider the need for specific clauses** - such as the European Union's standard contractual clauses.
- Data protection addendums (DPA) often only refer to the use of personal information (PI) or Personally Identifiable Information (PII). Depending on your company, **you may want to negotiate for breach notification requirements beyond PI/PII** (i.e., also for incidents that don't involve PI/PII) – for example, if the contracting party is a critical third party.

2. Consider language that requires notification within a timeframe:

- Consider inserting language that **requires a party to notify the other within a specific deadline** (for example, maximum 48 hours) in the event of actual or suspected unauthorized access or use of confidential information - especially if personal information is involved in the deal.
- Consider that your **third-party service provider may have a breach that affects many or all of its customers**, including your organization.
  - The agreement should address whether the service provider **will take on notification obligations**, for affected individuals, government agencies, media, etc.
  - In that case, the agreement should still **address timely reporting to your organization**. This is to enable you to prepare to address issues and questions relating to customers, employees, investors, etc.

- The agreement also should **address your role in the notification process**. Even if the service provider agrees to take on the notification process, **your organization may still be considered the owner of the data** and responsible for complying with the notification requirement. Negotiate some level of **review and approval**.

- **Consider the time** in which your company may in turn need to notify data subjects.

3. Consider insurance and costs of remediation:

- Consider whether to **require the other party to have cyber insurance** with certain minimum limits of coverage.
- Consider language **requiring a party to cooperate** in the event of a breach.
- Consider language **requiring the other party to bear the cost of remediation**, including, without limitation, notification costs.
- Consider **requiring an indemnification clause** related to cyber incidents and data breaches. Consider listing specific costs as covered – such as (without limitation) forensic review, data mining, notification letters, credit monitoring, and call center services.
  - Here is one example of a contract clause seeking first-party costs related to a breach *(reminder: the clause below is a sample for informative purposes only; it is not a model clause, and it doesn't constitute legal advice):*

    "To the extent any Security Incident is attributable to a breach of the obligations under this Agreement by Service Provider, including without limitation Service Provider's agents, subcontractors, assignees, or delegates, Service Provider shall bear the costs incurred by the Company to the extent it is necessary or appropriate for the Company to comply with its respective legal or other obligations relating to such breach under the applicable breach notification statute or regulation or any contract or other obligation, which shall include the following costs reasonably incurred in responding to such breach: (1) the cost of preparing and distributing notifications to affected individuals, (2) the cost of providing notice to government agencies, credit bureaus, and/or other required entities, (3) the cost of providing affected individuals with credit monitoring services for a specific period not to exceed twelve (12) months, or longer if required by law, (4) the cost of call center support for such affected individuals for a specific period not to exceed ninety (90) days from the date the breach notification is sent to such affected individuals, and (5) the cost of any other measures required under applicable law or any government enforcement authority, or deemed to be reasonable and appropriate by the Company."

4. Consider how robust your vendor's cybersecurity practices are:

- No matter what clauses you put in a contract, what matters is **what cybersecurity measures the vendor actually takes.**
- Consider whether the vendor **has a recognized certification** for its services or systems**,** such as, without limitation, ISO/IEC 27000, ISO 27001 Certification, PCI-DSS, ISAE3402/SOC1/SOC2-Type1/Type2, and Health Information Trust Alliance (HITRUST) Certification.
- For contracts that are mission-critical or that involve sharing sensitive business or personal information, consider asking the vendor to complete **a security due diligence questionnaire.**
- From a compliance perspective, **be sure this process is documented to** satisfy applicable legal requirements.
  - **For example, in the United States**, the ***Federal Department of Labor issued guidance in 2021 requiring retirement plan fiduciaries to assess the cybersecurity of service providers to their retirement plans***. Under such guidance, ERISA fiduciaries must be involved in this process, and need not be IT security professionals (ERISA is the US ***Employee Retirement Income Security Act***). But they must be prudent, which includes exercising their role as a fiduciary and documenting their efforts. Of course, vendor assessment requirements are not limited to an organization's retirement plans.
  - **For data processing subject to the EU GDPR or the UK GDPR**, the data processing agreement and any cross-border transfer mechanism such as the EU standard contractual clauses must contractually obligate the vendor or processor to implement reasonable safeguards.

5. Consider training employees on proper procurement practices:

- **Consider preparing a suitable template contract** with appropriate terms**.**
- **In addition, employees must know** that they have to use these templates and get these contracts signed, or that they must impose the required terms on vendors.
- Depending on how procurement is handled in your organization (centralized v. decentralized), **conduct training and education as needed** to ensure employees are aware that appropriate contract clauses must be imposed on relevant vendors.

TAKE ACTION: Write one or two steps that you plan to implement.	
Describe	By what date?
1.	
2.	
Notes:	

Learn more

- ***Operational Chaos: The Ramifications of a Vendor Data Breach***, by Jason C. Gavejian and Stephen T. Paterniti, Jackson Lewis P.C.
- ***4 Ways to Mitigate Vendor Cybersecurity Incidents***, by Kate Kreps and Elizabeth Burgin Waller
- ***Legal Tech: Navigating Indemnification Clauses in AI-Related Agreements***, by Olga V. Mack, Brian Mack, and Foster Sayers
- ***Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information***, by ACC

CHECKLIST 7

Artificial Intelligence and Cybersecurity

The rise of Artificial Intelligence introduces new cybersecurity challenges and threats, but also new opportunities to bolster an organization's cybersecurity.

1. New cyber threats posed by AI:

- AI poses new **risks of impersonation and fraud**, as tools may be used to create ***deepfakes*** – video or audio content that falsely uses someone's image or voice.
- Malicious actors might try to use or re-create such tools to impersonate your staff or business partners and engage in **phone or video communications and meetings**.
- They may create fake content that **falsely features your group or its staff** engaging in compromising conduct or speech.
- AI tools may be used by hackers, such as to develop **malicious code** or to craft **more convincing phishing email messages**.
- ***TIP:*** **Consider your authentication protocols**, for example, for verifying internal instructions to issue payments or to disclose sensitive information.
- ***TIP:*** **Ensure your staff members are regularly trained** to exercise appropriate caution when receiving email or text messages, clicking on links or attachments, or responding.
- ***TIP:*** In your crisis communication plans, **consider the scenario where someone publishes false content** that damages your company's reputation. While this may not be a cybersecurity issue per se, the damage may be significant.

2. Weaving cybersecurity into your business's approach to AI tools:

- **Assess the potential vulnerabilities** of the AI tools **your business** plans to use, and of AI tools **your third-party partners** are using (for example, vendors).
- **Assess how sensitive the data is** that will be processed through AI tools (confidential business information, personal information, etc.).
- **Ensure cybersecurity and data privacy are part of the analysis** when the business assesses the balance between the benefits and risks of using an AI tool.
- As part of your contracting practice, **consider requiring vendors to disclose** whether they are using AI tools and for what purposes.

- Ensure there are **adequate protections in place in your contracts** to mitigate cyber, privacy, and other types of risk (such as intellectual property risk).

3. Opportunities to enhance cybersecurity through AI:

- AI may be used to process **large volumes of information and discern patterns**.
- Consider opportunities to leverage AI tools to boost your cybersecurity, such as via **threat detection tools and alerts**. This type of tool likely falls within the portfolio of the Chief Information Security Officer (CISO) or the cybersecurity team rather than the General Counsel or the Legal Department. Have a conversation with the relevant stakeholder regarding how your organization uses or could benefit from such technology.

TAKE ACTION:
Write one or two steps that you plan to implement.

Describe	By what date?
1.	
2.	
Notes:	

Learn more

→ ***Developing a Privacy and Cybersecurity Training Program for Employees***
by Jackson Lewis P.C.

→ ***Cybersecurity Awareness Month Series: Employee Cybersecurity Awareness Training***
by Jackson Lewis P.C.

Connect with Peers and Boost Your Cyber Skills

Connect with the ACC IT, Privacy & e-Commerce Network

- Monthly **live discussions** with other in-house counsel and outside speakers.
- A dedicated **e-forum** to connect with peers and seek their insights.
- ***Join the Network!*** For ACC members only.
- Not an ACC member? ***Join ACC.***

Learn strategies at the ACC Foundation Cybersecurity Summit

- Learn about the **latest cyber threats and innovations** for in-house.
- Participate in **deep-dive sessions** with leading cybersecurity and in-house professionals.
- Discuss **emerging issues**, and tips for preventing and responding to data breaches.
- ***Learn more about ACC Foundation events***

Explore trends and tips at the ACC Annual Meeting

- **Enjoy** the largest annual gathering of the global in-house community.
- **Engage** in lively sessions and learn the latest in-house strategies, tips, and trends.
- **Bring** your in-house team. Get **CLE/CPD credits**.
- Enjoy the **unique experience** of our vibrant ACC in-house community.
- ***Learn More***

10 Insights on Cybersecurity Topics

1. *ACC Foundation State of Cybersecurity Report*
2. *Cybersecurity Basics for In-house Counsel*
   article by ACC
3. *What to Include in an Incident Response Plan*
   podcast by Jackson Lewis P.C.
4. *Importance of Protecting Employee Information as Privacy and Cybersecurity Laws Proliferate*
   article by Jackson Lewis P.C.
5. *Operational Chaos: The Ramifications of a Vendor Data Breach*
   podcast by Jackson Lewis P.C.
6. *Preparing Your Healthcare Organization for a Data Breach*
   podcast by Jackson Lewis P.C.
7. *Developing a Privacy and Cybersecurity Training Program for Employees*
   article by Jackson Lewis P.C.
8. *4 Ways to Mitigate Vendor Cybersecurity Incidents*
   article by Kate Kreps and Elizabeth Burgin Waller
9. *Legal Tech: The Crucial Role of Legal Stewardship During the AI Revolution*
   article by Olga V. Mack, Kevin Keller, and Kristina Podnar
10. *Why Cybercriminals Love the Work-from-home Era*
    article by Helena Sousa Aguiar

7 Sample Tools, Forms, and Checklists

1. *Ten Key Items to Strengthen Preparedness for Data Incident Response*, a checklist
   by Jackson Lewis P.C.
2. *Data Breach Checklist*
3. *Data Breach Notification Chart*
   by Jackson Lewis P.C.
4. *Sample Notice of Data Breach Letter (US)*, by Jackson Lewis P.C.
5. *HIPAA Security Incident Assessment Tool*
   by Jackson Lewis P.C.
6. *Checklist: Ransomware Attacks - Prevention and Preparedness (US)*
   by Jackson Lewis P.C.
7. *Cyber Incident & Data Breach Management Workflow*
   by Exterro

More Resources

1. ***Visit the ACC Resource Library. Find thousands of resources:***
   - Sample contracts and policies
   - Checklists and articles
   - ACC in-house survey reports
2. ***Explore ACC Curated Collections:***
   - *Artificial Intelligence*
   - *Privacy and Cybersecurity*
   - *ESG (Environmental, Social, and Governance)*
   - *Teaching Law School*
   - *New to In-house Resource Center*

