Baker McKenzie.

So You Think You Want To...

Be cyber resilient and cyber ready

Cybersecurity

How it affects your consumer goods & retail business

The consumer goods & retail (CG&R) sector is a prime target for cyberattacks due to massive volumes of customer data, employee personal data, and other sensitive digital information that global companies now deal with across multiple jurisdictions on a daily basis (e.g., names, addresses, dates of birth, biometrics, measurements, payment card information, and customer loyalty data across store networks). Business disruption and operational impacts on manufacturing and sales also make CG&R businesses attractive targets for malicious actors. Not to mention the IP related assets that can be compromised, like trade secrets (information on products or services, suppliers' information, internal procedures which are intrinsic to a brand's DNA like selling ceremony, etc.).

Businesses face the challenge of protecting against diverse and ever-changing threats to the security of their business-critical information and systems, as well as navigating through changing legal frameworks which govern the digital economy.

Risks include:

- Attackers targeting the weakest link in your network or an international supply chain – a supply chain attack might disable a third party system that is critical for your day-to-day operations, or compromise sensitive data held by your supplier.
- Rogue employees stealing, deleting or interfering with customer or other company data.
- Genuine errors by employees responding to elaborate phishing or spear attacks.

The risks to CG&R companies in the context of a cybersecurity incident are significant and include:

- Regulatory action.
- Class actions and other claims from consumers, investors, corporate customers, employees, and others.
- Business interruption and distraction.
- Adverse media attention and reputational harm, with detriment to brand image and trust.

Strong understanding of cyber risk and resilience at the board level is imperative, with regulators imposing new requirements that boards exercise oversight of cyber risks.

Companies that create and implement a proactive cyber response plan should address the three main phases of cyber resilience –preparation, reaction during the incident and post-incident actions.

By establishing a sound and well tested cyber response plan, a CG&R company can achieve:

- Defensive measures to defend and (when it happens) limit the negative impact of a cyber attack.
- More certainty for growth in the digital economy.
- Mitigation of risk when a cyber security incident does occur. This is particularly effective in light of liability of the company when addressing post-incident litigation (i.e. regulatory authorities, class actions, customers' claims, etc.).
- Enrichment of relationships with customers, suppliers and employees.

Conversely, poor cybersecurity and data protection policies erode consumer trust and jeopardize business relationships, especially where a company's level of compliance and security measures are not aligned with those of its business partners and the established reputation of a brand on the market.

Growing digitization of businesses has meant that the legal and business risks associated with non-compliance with developing regulatory regimes have escalated. In particular, in the CG&R industry, it is important to understand how to comply, and demonstrate compliance with, payments industry requirements and standards such as Payment Card Industry Data Security Standard.

Companies that create and implement a proactive cyber response plan should address the three main phases of cyber resilience – preparation, reaction during the incident and post-incident actions.

Pro tips for CG&R companies to ensure they are cyber resilient and ready

People
Engage key stakeholders in training to better identify and respond to cyber risks.

Process
Create an actionable incident response plan that incorporates trusted partners and vendors who can provide legal and technical support during and after a cyber attack.

Technology
Stay up to date on cyber risks that impact your technology, operations, brand and industry, as well as actions you can take to mitigate those risks.

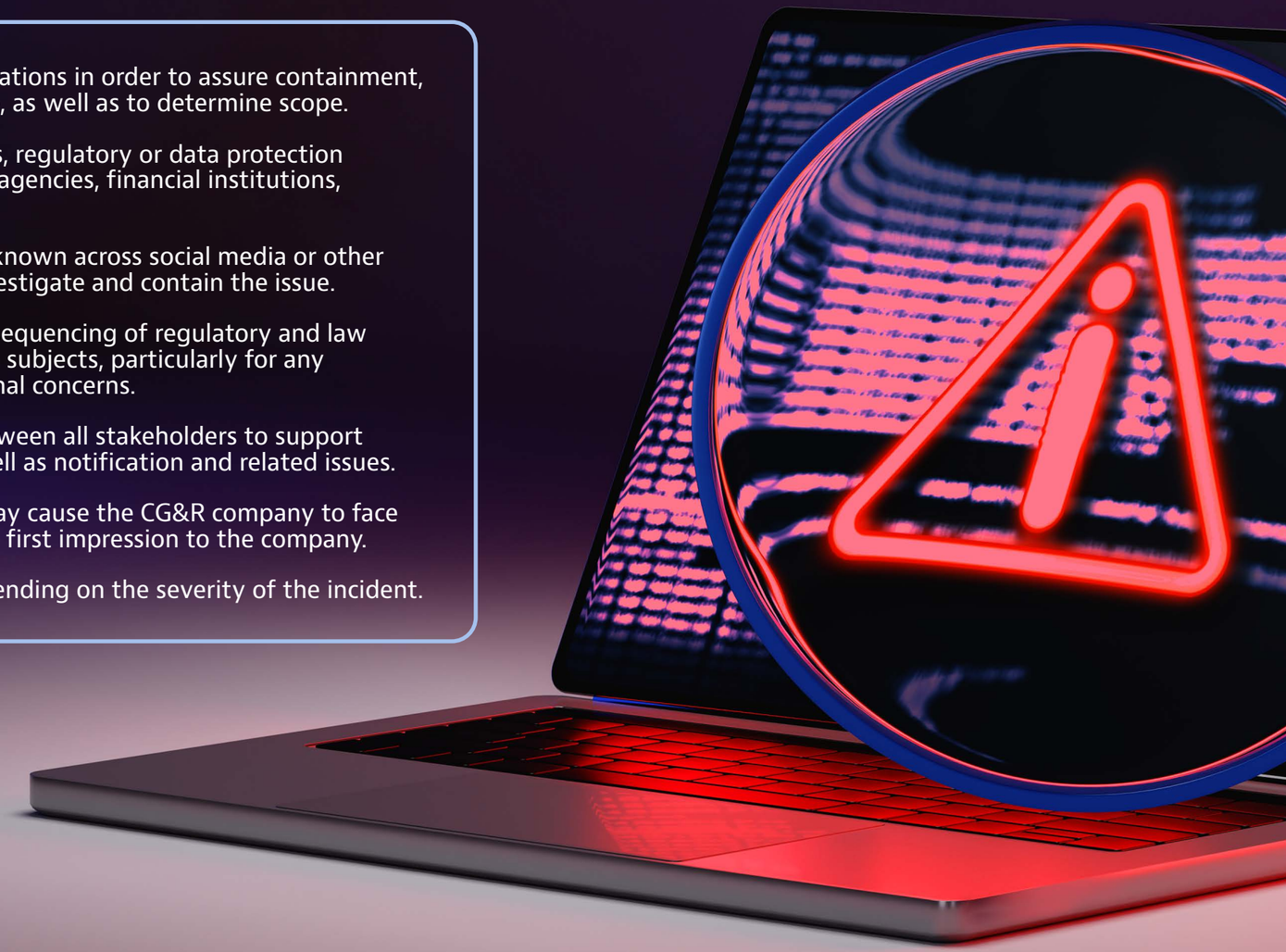
Preparation

From the get-go

- Develop, review and refine a cybersecurity incident response and breach notification plan.
- Ensure appropriate board engagement and oversight of cyber threats, supported by the right expertise.
- Identify customer touchpoints and map the type of sensitive personal data (e.g., health or medical, financial, national identifiers, or the like) and highly confidential business information that you obtain and consider whether collection and use could be minimized or other protections implemented.
- Consider what is required from your suppliers (e.g., conducting audits, maintaining up-to-date software security patches, obtaining warranties or indemnities from the supply chain, etc.).
- Identify areas of vulnerability and degrees of risk accounting or regulatory obligations owed across jurisdictions including Federal Trade Commission, Information Commissioner's Office, Serious Fraud Office, Financial Conduct Authority, Prudential Regulation Authority, Department of Financial Services and state regulators.
- Test the adequacy of systems and controls by reviewing your existing policies and their application.
- Update record retention and secure deletion policies and schedules.
  Ensure internal guidance and training for all staff is regularly conducted.
- Identify broader potential implications for reputation, criminal and civil litigation exposure, employees and investor relations that may flow from any regulatory report.
- Conduct regular information security and data protection or privacy assessments, and establish appropriate controls including file encryption and user authentication requirements.
- Conduct table top or other mock drills with a crisis management team to test responses within the 24-hour news cycle.

Investigation & Crisis Management

- Many jurisdictions require the company to undertake urgent investigations in order to assure containment, preserve evidence, and implement remediation to prevent recurrence, as well as to determine scope.
- Many jurisdictions also require mandatory notifications to individuals, regulatory or data protection authorities, the media, law enforcement authorities, credit reporting agencies, financial institutions, investors and others.
- Time pressure becomes acute if the data security incident is already known across social media or other public channels before the CG&R company has an opportunity to investigate and contain the issue.
- Critical steps include close coordination globally on the content and sequencing of regulatory and law enforcement reporting as well as notifications owed to affected data subjects, particularly for any incidents that may mature into class actions or other multijurisdictional concerns.
- Other essential aspects include effective internal communication between all stakeholders to support informed decision-making on performance of the investigation as well as notification and related issues.
- Business interruption and other aspects of cybersecurity incidents may cause the CG&R company to face challenging risk balancing issues, such as ransom demands, which are first impression to the company.
- Senior management and board engagement may also be critical depending on the severity of the incident.



Post Event

What's next for the CG&R company?

- Promptly and vigorously address regulatory inquiries, class actions, or other claims.
- Remediate against future breaches including through the establishment of appropriate policies and procedures on information security. Some jurisdictions compel companies to fulfill this step.
- Capture lessons learned, documentation and ongoing remediation.
- Refine current approaches and policies following lessons learned from any breach.
- Report internally to the board.
- Anticipate future attacks.
- Continue to pay attention to privilege issues through technical reports and further due diligence.

Things to expect

- Anticipate follow-on inquiries from data protection, consumer protection, labor or other authorities and potential litigation.
- Expect heightened scrutiny over:
  - Information security and remediation to remove 'root cause'
  - Privacy compliance programs

Dos and Don'ts

In the event of a cyber incident

Dos

- Activate the incident response policy.
- Take timely steps to mitigate the harm of a data breach.
- Engage relevant stakeholders.
- Level set on privilege issues.
- Conduct a diligent investigation of the facts.
- Conduct a proper gathering of data (e.g., chain of custody).
- Consider broad personally identifiable information (PII) definitions.
- Consider any notification obligations beyond privacy (e.g., contractual obligations, consumer protection, SEC reporting).
- Provide accurate and timely notifications to proper parties and in the proper order (e.g., merchant banks or card brands, law enforcement, government authorities, individuals, consumer reporting agencies, insurers, and/or investors).
- Respond promptly to government authorities and press.
- Assure clear communication to stay "on message" across all regions (e.g., government filing forms).

Don'ts

- Notify before developing a sufficient knowledge of the facts ("ready, fire, aim" is not a good strategy).
- Create or share communications without reference to privilege.
- Engage in decision-making in silos.
- Act inconsistently with privacy, confidentiality, secrecy, or other data regulations in the conduct of the investigation (e.g., cross-border transfers).
- Permit local control over messaging.

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com