Into the Cyber-Breach:

How CLOs Build Organizational Resilience and Lead During Crises

LexMundi
World Ready

Table of Contents

About This Report

The risk of corporate cyber-breaches has become not just a potentiality but an eventuality with severe implications for basic business continuity and significant liabilities related to preemptive (in) action and post-breach responsiveness. As multinational enterprises embed information technology deeper and deeper into operations, products and services, they face unforeseeable cyber-security vulnerabilities that expose management systems as well as critical physical and intellectual assets to this inevitable cyber-breach risk. Beyond the immediate damages resulting from data loss, companies must also prepare for a tailspin of consumer confidence, reputational problems, stock devaluation, credit downgrades and costly regulatory investigations.

One of the most difficult challenges in dealing with cyber-risk is the need to coordinate a wide scale response across jurisdictions due, in most part, to the following factors:

1. The borderless nature of cyber-threats coming from anywhere and exposing the organization everywhere.
2. The web of incompatible regulations across jurisdictions, in which data protection authorities cue one another and are not necessarily bound by legal privilege.
3. The extensive consequences of and liability for breaches.

The complexity of coordinating global responses to cyber-breaches led the experts who worked on the 2017 Lex Mundi Summit to focus on the overarching theme of building organizational resilience and providing leadership during crises. This report analyzes insights and best practices shared by general counsel participants during the tenth annual Lex Mundi Summit in Amsterdam, which highlighted three broad ways that general counsel contribute to organizational resilience and provide leadership:

1. Strengthening resistance to attack through basic cyber-hygiene
2. Preparing to respond to the inevitable cyber-crisis
3. Adapting the legal department to permanent cyber-vulnerability

This report includes contributions from Summit speakers covering the global threat landscape, the evolving web of regulation, the challenges posed by data-privacy regimes and general guidance for communicating in times of cyber-crises.

Lex Mundi's Cyber-Breach resources can be found online at www.lexmundi.com/cyber-security, consisting of a comparison of Data Privacy notification requirements across jurisdictions and experts around the world who can form part of a client's rapid reaction force.

We extend our thanks and appreciation to general counsel participants, Lex Mundi member firm lawyers and our guest speakers for their contributions to the program and their active Summit participation.

We hope you find this analysis beneficial and look forward to the 2018 Lex Mundi Summit in Amsterdam (June 7–8).

Eric R. Staal
Director, Business Development

Carl Anduri
President

Lex Mundi Global Cyber-Breach Resources
Complimentary Access: **www.lexmundi.com/Cyber-Security**

Lex Mundi Summit Report: Best Practices for Coordinating the Global Response

In response to the problem of increasing cyber-vulnerability, discussions at the 2017 Lex Mundi Summit focused on best-practices to support organizational resilience and leadership in three broad areas:

1. Strengthening resistance through cyber-hygiene
2. Preparing to respond to the inevitable cyber-crisis
3. Adapting the legal department to permanent cyber-vulnerability

Strengthening Resistance through Cyber-Hygiene

The mindset that cyber-security is a matter for the IT department is long past. With the increased sophistication and far-reaching consequences of cyber-attacks, the issue is an increasing fiduciary responsibility assumed by the Board of Directors and falls under the oversight of legal, risk and compliance.

In particular, it is crucial that Board members and the C-suite are all committed to the prioritization of cyber-security as a one of the most important areas of business risk. One Summit participant articulated the difficulty posed by competing priorities: "Time to market and time to revenue are challenges all companies face, and they run against the grain of taking into account and securing against cyber- threats."

Summit participants acknowledged that the effectiveness of cyber-security strategy depends on a cross-functional approach[1] and provided examples of how they see this working within their own organizations:

- One company cited its cyber-security team, which consists of IT, compliance, legal and manufacturing to handle data breach procedures and incidents.
- Another company involved assigns the lead role for different phases to different functions, e.g. IT leads the advice in the first phase, legal leads action steps in the second phase and the C-suite leads decisions in the third phase.
- A third example was of a company in which compliance and data privacy departments report to the legal department, while the legal and IT departments collaborate on the incident response and data breach procedures.

[1] Crowdstrike, "Cyber Attack Survival Checklist," https://www.crowdstrike.com/resources/white-papers/cyber-attack-survival-checklist/.

The SANS Institute, a cooperative research and education organization specializing in information security, advises corporations to go a step further and appoint a corporate champion to oversee cross-functional teams that spearhead cyber-security initiatives. Seen as the most critical step in internal organizational resilience according to SANS, this champion implements risk policies and procedures resulting from the work of the cyber-security teams and advocates to the C-suite for approvals.[2]

One of the first steps of the interdisciplinary teams is to conduct a cyber-threat intelligence (CTI) assessment to enhance the knowledge and understanding of what are the 'crown jewels' in terms of corporate assets, who is a threat and what are their goals. "[T]he perception of (C) TI is turning from one of luxury to necessity as information security professionals come to realize that attackers often have a better understanding of their organization's networks than they do."[3]

One corporate counsel panelist at the Summit advised the audience to employ an in-house hacker to conduct an internal CTI review by hacking the enterprise system to identify vulnerabilities. Another panelist recommended collaborating with common industry-specific public and private sector groups to share information on who is hacking and how, as part of an external CTI evaluation. CTI assessments are conducted in a multitude of ways including the hiring of external experts. The consensus among Summit participants was that the information gleaned is invaluable to determining organizational sensitivities and prioritizing threats.

A particular vulnerability is a company's vendors and third-party suppliers, which open up multiple external avenues for hackers to access the enterprise's internal systems. As seen with Target, Home Depot and most recently Verizon, third-party vendors represent one of the weakest links in an organization's cyber-resilience whether it be through employee error or a hacker leveraging access through third-party credentials. To minimize these risks, corporations must conduct extensive due diligence of vendors and regularly conduct audits to ensure internal and external compliance. Contracts should also be in place outlining liability should a breach occur. One Summit participant encourages negotiation with vendors since vendor acceptance of unlimited liability can raise red flags about the seriousness of the commitment to security.

Some corporations choose to enhance their cyber-hygiene through cyber-attack insurance. However, the Summit participants had differing viewpoints on the actual benefits of insurance. Some saw it as leading to a false sense of security; others saw the insurance coverage qualification process in itself as a way to mitigate risk by forcing companies to conduct thorough assessments and implement countermeasures. A recent article written for the ABA Journal demonstrates a third viewpoint advocating for the acquisition of insurance in reference to the DLA Piper attack, citing that cyber-attack insurance could provide coverage for loss of income, expenses and expert hiring.[4] Coverage adequacy and effectiveness aside, insurance policies can have positive reputational externalities reflecting a commitment to preemptive action to protect data, which lends assurance to customers and business partners when incidents occur.

Best Practices

- Ensure directors of Boards and members of the C-suite commit to cyber-security and are kept regularly informed.
- Integrate IT, Legal and Communications into a cross-functional cyber-security team.
- Conduct cyber-threat intelligence (CTI) assessments.
- Assign responsibility for monitoring the threat landscape to a range of staff to make it less likely that critical aspects will be missed.
- Explore additional security measures including credential leak alerting services.
- Mitigate internal risk by establishing internal policies restricting access to certain websites and installing VPNs.
- Provide regular employee training on cyber-security risks and procedures.
- Conduct extensive and regular due diligence of third party vendors.
- Consider cyber-risk insurance or, at a minimum, implement the measures required to qualify.

[2] Benjamin Wright, *Complying with Data Protection Law in a Changing World* (SANS Institute, June 2017), 10-11.

[3] Matt Bromiley, *Threat Intelligence: What It Is, and How to Use It Effectively* (SANS Institute, September 2016), 3.

[4] Debra Cassens Weiss, "Costs of malware attack on DLA Piper could be in the millions; does insurance cover it?," *ABA Journal*, July 10, 2017, http://www.abajournal.com/news/article/costs_of_ransomware_attack_on_dla_piper_could_be_in_the_millions_does_insur.

Preparing to Respond to the Inevitable Cyber-Crisis

Few events can destroy corporate reputation faster than a poorly handled cyber-attack. Both Yahoo and TalkTalk, to name a few, prove how the lack of a clear incident response plan can lead to stock devaluation, executive resignations, and hefty fines. The highly-publicized Yahoo case further exemplifies how poor security response protocols can ultimately lead to demise. "An inadequate response to a breach, not only by the technology team but also from the marketing, public affairs, or customer service functions, can be as damaging as the breach itself."[5] Protecting the corporate reputation in the face of a cyber-breach depends on a comprehensive response.

Much like cyber-attacks, incident response plans are not one size fits all. Response plans vary by industry and information acquired during the CTI assessment. "The primary objective of an IR (incident response) plan is to manage a cyber-security event or incident in a way that limits damage, increases confidence of external stakeholders, and reduces recovery time and cost."[6] Beyond a strict definition of incident response, one Summit participant stressed the importance of counteroffensive measures in preventing the enterprise from being seen as the "bad guy."

Source: Brunswick Group

Take these steps now to PREPARE for an incident:

Build Trust.
Communicate with honesty and transparency before, during, and after a crisis in order to build trust and maintain a reputation for integrity.

Map Your Stakeholder Universe.
Understand all of your stakeholders and how to manage those relationships in times of crisis. Communicating to the right people at the right time, in plain language, will get you a long way.

Educate Employees.
System penetrations are often the result of an employee, or the company, failing to follow its own procedures. Ongoing education is essential.

Understand Your Organization.
To execute an effective response you must first understand your organization, existing processes, and how information is shared within and across departments. Misunderstanding these connections can derail an incident response.

"No war plan survives once the shooting starts, but preparations and protocols are valuable."

Response plans should be multifaceted including a situational analysis and reaction for breaches of different types of data (i.e. customer information, intellectual property, security protocols, etc.). This data should be prioritized to determine which areas are most critical to protect, given that full protection against a cyber-attack is almost impossible. While it is difficult to foresee what shape a crisis could take, Summit participants determined that the most effective plans account for both small and large crises and allow for adaptation once attacks occur. No war plan survives once the shooting starts, but preparations and protocols are valuable.

A key challenge is to ensure an enterprise-wide roll-out of measures and plans across borders and business units. Summit participants recommended simulations and tabletop exercises to engrain incident response plans into the corporate culture. "Working through roles, responsibilities, and the steps of a complete IR plan prepares a team for action and quickly identifies any weaknesses in your plan, processes, data collection efforts, and team capabilities."[7] McKinsey & Company formalized this approach in their cyber-incident response article with a three-step process including: 1) making the plan easily accessible; 2) increasing awareness through communications and training; and 3) conducting war games.[8] One Summit panelist also reinforced the idea of cyber-security strategies as needing to be agile. The fluidity of cyber-risks and the increased sophistication of hackers requires these strategies to be continually updated.

[5] James Kaplan and Jim Boehm, "At the core of your cybersecurity strategy: Knowing your capabilities," in *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities* by Domenic Antonucci (John Wiley & Sons, 2017), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-blog/at-the-core-of-your-cybersecurity-strategy-knowing-your-capabilities.

[6] Tucker Bailey, Josh Brandley, and James Kaplan, "How good is your cyberincident-response plan?," McKinsey & Company (December 2013), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan.

[7] Crowdstrike, "Cyber Attack Survival Checklist."

[8] Bailey, Brandley and Kaplan, "Cyberincident-response."

Case Studies

Yahoo: Yahoo chose to delay its public statements regarding the breach until all the facts were collected. Corporate level resignations ensued including the general counsel as well as the sale price reduction of $350 million to Verizon.

Sony: Sony did not acknowledge the breach and did not make any public statements. The US government finally intervened and made the disclosure. In the end, the CEO resigned over the incident.

TalkTalk: The CEO of TalkTalk disclosed the breach prematurely to the public stating that the breach was terror-related and affected the entire customer base, which negatively impacted its stock price. The full investigation later showed that the damage had been limited to three to four percent of customer data, and the source was a teenager in Northern Ireland. TalkTalk paid record high fines and experienced high executive turnover after the incident.

When a cyber-breach does occur, the first twenty-four to seventy-two hours can determine the fate of an enterprise's public reputation. To complicate matters, the European Union's General Data Privacy Regulation has a 72-hour notification requirement, but Summit participants were unanimous that a factual assessment of risks and damage inevitably takes longer. Summit participants debated how soon to make a statement, citing the Sony and TalkTalk cases as damaging examples at opposite ends of a spectrum: executives of the former avoided public comment while the media frenzied over disclosures, while the CEO of the latter prematurely speculated about facts in ways that led to significant financial losses and cost her own job.

Those participants advocating for a relatively quick public notification did concede that one must also take account of whether doing so might tip off hackers to countermeasures, efforts to trace them, and law enforcement action. As most information acquired in the immediate aftermath of a breach is unreliable, there was also agreement not to comment on aspects that have not been verified and only to state what is known.

Pre-determined messaging should put the focus on addressing the concerns of the public and corporate stakeholders. Four communication principles that will help protect integrity are: 1) to put the customer first, 2) avoid excessive communication (starve the fire of oxygen), 3) coordinate across major functions and, not least, 4) avoid saying too much, too soon and too confidently.

In terms of public perceptions, how corporations go about public notification is as important as the information that is communicated. At the Lex Mundi Summit, the Brunswick Group participants emphasized the obvious need for authenticity in all communications and suggested appointing an internal spokesperson to

Establish GUIDING PRINCIPLES to anchor decision making in a crisis:

1. **Put Customers First.**
By placing customers at the center of decision making, companies tend to make better decisions, limiting the damage of an incident. Preserve your current clients' willingness to transact with you, as well as your ability to attract new clients.

2. **Limit the News Cycles.**
Be thoughtful about how often you put out information that will draw attention to the incident. Over-communicating and correcting previous statements can make it appear that the response is not being effectively managed. Announcements should be thoughtful, consistent, and focused on actionable information.

3. **Be Coordinated.**
Multiple departments must work together to ensure a smooth, consistent response. There are also multiple stakeholder groups that will require attention simultaneously. Find a process for coordination that works for your company and stick to it.

4. **Be Authentic.**
Remain true to your brand voice and values. There will be legal constraints on what you can say and technical details to get right, but at its core a cyber incident is a human event. Whenever possible, speak in clear language that humanizes the incident and your response.

Source: Brunswick Group

Who is in your STAKEHOLDER universe?

Source: Brunswick Group

reinforce the image of handling the crisis. This person should be personable and comfortable in the public eye, but not the CEO. Brunswick explained that the CEO is better held in reserve for when the crisis escalates to a point that it is necessary to utilize a more impactful player.

Best Practices

- Use natural disaster plans or other crisis management plans as frameworks for incident response protocols.
- Develop plans that include small and large crises that can be tailored when a breach occurs.
- Conduct simulation exercises to improve crisis management skills and plans.
- Establish protocols and criteria for when to notify the public and authorities.
- Draft talking points that relay the commitment to protecting customers, employees, shareholders and assets.
- Call upon the authorities to help with the threat response and pursuit of the criminals.
- General counsel, acting as the cyber-crisis captains, need to communicate in non-legalese (e.g. focus on commitment to protecting customers rather than advocating against the company's culpability).
- Build trust and reputation for integrity by communicating with truth and transparency before, during and after the crisis while remaining aware of the dangers of over communication and the "starving the fire of oxygen" approach.
- Designate one person to manage the mandatory regulatory notification processes.

Adapting the Legal Function to Permanent Cyber-Vulnerability

Lex Mundi Summit participants acknowledged that corporate leaders tend to default to the general counsel during a cyber-crisis. Speakers described a chaos situation with multiple workstreams going in different directions, external relations pressing to communicate in a timely fashion, and fact-gathering only just beginning. People need to know what role they have and, crucially, what roles they don't have.

This environment has shifted the role of the general counsel and the legal department from one of a sideline advisor to a lead player in the development and implementation of cyber-security measures. As seen in the Yahoo case, those that do not adapt could put their job and their company at risk. Enterprises that wait until after the breach occurs to involve the general counsel open themselves to myriad problems. In an effort to contain the breach, managers unfamiliar with discovery and litigation proceedings can mistakenly destroy evidence, inadvertently waive legal privilege, or allow proprietary information to fall into the wrong hands.

Summit participants discussed going beyond collaboration on cyber-security policy and crisis preparation to having members of the legal and IT teams work side-by-side. Some had hired a Chief Information Security Officer (CISO) that reported directly to the general counsel; others had a head of legal for IT whose role is to connect the dots across IT, privacy, IP, litigation, risk and compliance, etc. Another model, which seems to be increasingly frequent, is to have a Global or Chief Privacy Officer.

Regardless of the approach, the participants agreed that the legal department should work closely with the IT department on the CTI assessments as well as on the regular updating of countermeasures. Following the Yahoo case, there was even speculation that the role of the in-house counsel was generally at risk if he or she is unable to "escalate these [cyber-security] issues within the legal department and within

the organization."[9] This communication can only be had if the general counsel and the legal department understand the cyber-security procedures and policies in place before, during and after a breach.

The general counsel has the responsibility to educate and advise the C-suite and Board on the importance of robust cyber-security response plans. "The possibilities of a cyber-attack must be integrated with other risk analyses and presented in relevant management and board discussions. [T]he implications of digital resilience should be integrated into a broad set of governance functions such as human resources, vendor management, and compliance."[10] It is the Board of Directors and executive level that determine a corporation's approach to cyber-security and integration into the corporate culture.

One stumbling block to getting the culture right at the top of the organization is communication. As one Summit participant explained, "Board members most often are not cyber-natives. They require information and support to manage cyber-security and incident response plans." One recommendation when speaking with the C-suite and the Board is to "avoid confusing cyber-security jargon and focus instead on understanding the various management goals at play."[11] Clear and focused messaging can assist in overcoming the technical language barrier and ensure that the executives and Board understand the fundamental risk potentially facing the enterprise.

The above measures only scratch the surface for the role that the legal department of the future will play in cyber-security risk management. As technology itself becomes more and more integral to business, it is conceivable the legal department not only appoints a Legal Head of IT, or even a team to handle legal IT, but that cyber-security simply becomes part of every in-house lawyer's job similar to the way that all members of the legal department approach their roles with an eye on compliance or on overall mitigation of liability.

Finally, a critical observation emerged that the legal profession (in-house counsel and private practitioners) should play a role in shaping the way governments react to cyber-breaches. Regardless of the number of security measures implemented to protect data, governments hold corporations accountable when a cyber-breach occurs instead of focusing on prosecuting the criminals responsible. One corporate counsel emphasized this point when she explained that her company has reported the identity and the address of cyber-hackers to the authorities many times with no resulting actions." [C]yber-attacks are just a 21st century version of theft," stated another corporate counsel panelist. Further to the point, some Summit participants wanted companies to be empowered to engage in the pursuit of cyber-criminals through both public and private remedies, specifically through recourse to criminal indictments under the Uniform Trade Secrets Act and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctions. The law remains undeveloped in this area, and the participants agreed that both the laws and the sanctions will become more robust over the next ten years.

Best Practices

- Ensure a strong role for the general counsel or a senior member of the in-house legal team in the formulation and implementation of cyber-policies and response plans.
- Integrate cyber-risk as an overall part of business risk and governance.
- Avoid confusing technical language when discussing cyber-security measures with internal and external shareholders.
- Quantify risk and security improvements for the executive team and Board of Directors.

Conclusion

The borderless nature of cyber-threats, the web of regulation across jurisdictions and the extensive damage resulting from breaches all require companies to build resilience and vigilantly prepare for crises. The insights and experience shared by corporate counsel and other participants at the 2017 Lex Mundi Summit yielded a roadmap for general counsel to take more responsibility and to play a more active role in better preparing their company for the inevitable breach.

[9] Jennifer Williams Alvarez, "After Yahoo, Are In-House Counsel Jobs at Risk Over Cybersecurity?," *Corporate Counsel*, (March 2, 2017), https://www.law.com/corpcounsel/almID/1202780379239/.

[10] Kaplan and Boehm, "Cybersecurity strategy."

[11] Jeff Stone, "How Boards Should Talk about Cyberrisk," *Wall Street Journal*, (April 4, 2017), https://www.wsj.com/articles/how-boards-should-talk-about-cyberrisk-1491305353?mg=prod/accounts-wsj.

The Global Cyber-Risk Landscape: Understanding the Threats

Recent events emphasize that cyber-security risks are becoming more prevalent, and there is no reason to believe that we will see a decrease in the future. Rather than delegate the responsibility of managing the risk solely to the technical experts (i.e. CIO, CISO), it is highly recommended that enterprises integrate cyber-security risk into the normal business risk discussions and implement processes to monitor this risk at the C-suite and Board levels.

Both personal and professional technological advancements have left society open to greater and more sophisticated cyber-attacks:

1. A Connected Society – The Internet of Everything

Our society, economy, democracy and private lives all depend more and more on information obtained through the internet. For example, critical infrastructures are operated remotely, intelligent homes communicate with residents and control stations, personal and professional interactions are digitized and cars will soon be self-driving. And, our whole infrastructure is moving to the cloud.

Our dependence on information and communication technology is drastically increasing, which means an increased exposure to the threats coming from and over the internet.

2. Intrinsically Vulnerable Systems

Currently, it is almost impossible to build a system that is not intrinsically vulnerable, and built-in security is a remote dream, resulting in systems that are fragile and breakable. The infrastructure we use is becoming increasingly complex, and the attack surface is growing exponentially.

Our infrastructure is also often managed by others – cloud providers, internet service providers and built-in devices. This system puts a substantial portion of the devices on which we depend outside of our control, drastically increasing a corporation's exposure to risk if those providers do not have patches available when vulnerabilities arise.

3. Well-Organized Adversaries

Our adversaries are well-organized, highly trained professional groups searching for vulnerabilities, using automated tools and developing exploits in an industrialized fashion. They have a well-functioning market for vulnerabilities, hacking tools and breaches.

Furthermore, vulnerabilities publicized by the vendors or leaked from breaches are weaponized by our adversaries faster than we are able to patch our systems. This situation leads to a proliferation of sophisticated cyber-weapons, making them available to less sophisticated state actors and cyber-criminals alike.

Examples of Current Important Threats

- Cyber-criminals have started to attack banks rather than the bank's clients. The Bangladesh Central Bank heist, one of the most visible examples, demonstrates the abuse of the SWIFT system to hack the clients. Some of these attacks are reported to have a state-sponsored origin such as North Korea.
- Ransomware incidents have dramatically increased, in some cases disrupting the function of critical infrastructure (hospitals, telecom operators). These attacks are becoming more sophisticated and more targeted.
- What is thought to be a Russian nexus group continues to aggressively attack governmental and private organizations for traditional espionage, but they also interfere openly in democratic processes. Disruptive cyber-attacks against critical infrastructure (electricity grid) in Ukraine have also been conducted.

What to do to improve our preparedness?

Most cyber-attacks are still initiated by phishing or spear phishing emails, stealing the victim's credentials or infecting his/her computer through interaction with the victim. Even though these methods are well known, they have a substantial success rate with a double-digit percentage of users succumbing to these attacks. Raising awareness can improve these numbers. However, the level of sophistication of these attacks is also increasing, so it is safe to always assume a breach will occur.

In such a scenario, any organization needs to take appropriate steps to be prepared for the unavoidable:

- Raise awareness and train C-suite and Board levels;
- Inventory and document key assets and perform a risk assessment, integrating the cyber-risk into the normal business risk assessment. Implement processes to monitor and report the risk at C-suite and Board levels;
- Protect assets, including reputational value, according to the risk, increasing the level of prevention for the most important assets;
- Invest in threat intelligence, detection and response. Develop response plans and practice implementing them.
- Prepare for compliance with breach legislation (EU NIS Directive, GDPR, sectorial regulations); and
- Interact with sector peers to learn and share experiences.

Cyber-attacks cannot be considered rare events any more, nor should they be considered as reserved territory for the technically skilled departments in an organization. Cyber-security risk should be made visible, understandable and manageable at the C-suite and the Board levels.

Contributed by: **Freddy Dezeure**
Former Head of CERT-EU (Computer Emergency Response Team)

The Evolving Regulatory Environment

The recent ALM "General Counsel Up-At-Night" survey[1] tells us that privacy and data security are among the top concerns of in-house legal departments today. This fact is not entirely surprising as high-profile security incidents have dominated news headlines. At the same time, enhanced global regulatory regimes have created a complex matrix of requirements with which global companies must comply.

Recent legal developments

Traditionally companies predominantly looked towards U.S. laws in regard to data breach notification obligations, as the U.S. had legal requirements addressing security related incidents. Currently, many countries around the world have started to amend their laws in response to increased cyber-security threats, and the number of jurisdictions in which notification may be required has steeply increased. Furthermore, legal obligations are no longer just about providing notification; more and more laws (also) introduce obligations around incident preparedness and cyber-resilience.

Indicating that cyber-security and incident response is one of the key-topics of this time, the European Union, as one of the more recently updated regulatory regimes, has addressed cyber-security in a variety of ways. While only a few European countries at present have codified breach notification in national law (some of which even take a voluntary approach), the upcoming General Data Protection Regulation (GDPR) will introduce a uniform requirement to provide notice to individuals and/or data protection authorities in certain events of loss or unauthorized use of personal information. Failure to give notice where required will be subject to a potential fine of up to 10 million Euros or 2% of a company's annual worldwide revenue (whichever amount would be higher). This fine is independent of any liability for potential third-party claims from individuals whose data was compromised.

Moreover, acknowledging that it is not just personal information that is of interest to bad actors, countries are increasingly looking to address potential vulnerabilities in other areas, such as financial disclosure laws and criminal reporting obligations around export control regulations, or regulating specific sectors that are considered to consist of a country's critical infrastructure (such as power grids or financial markets as well as the IT systems that support these infrastructures).

[1] ALM Intelligence and Morrison & Foerster LLP, "General Counsel Up-At-Night Report," (2017), https://media2.mofo.com/documents/170622-gc-up-at-night-report.pdf.

What can companies do to become more cyber-resilient?

Experience has shown that maintaining a detailed plan to drive the discussion and build consensus before an attack is the key to ensuring that, where possible, a cyber-incident doesn't turn into a crisis. However, having the plan alone is not sufficient; equally (if not more so) important is testing and training to execute the plan in the context of a (simulated) breach.

Other practical lessons-learned from recent cyber-security incidents include:

- Avoid having too many responsible parties with unclear decision-making paths
- Ensure that the incident response team has the appropriate authority and mandate to make decisions, while at the same time knowing which decisions require escalation
- Ensure that the response team has the appropriate skills and ability to coordinate their efforts and responsibilities
- Make sure that the incident response process is well thought out and fits the realities of your company
- Especially in cyber-incidents that are cross-border: make sure your efforts are aligned and coordinated.

Cyber-Security and the Board

Finally, we are seeing more and more that the C-suite and Boards of Directors request to be updated periodically about a company's cyber-security threat landscape and resilience. This development is commensurate with the fact that having involvement and backing at this level is imperative for a company's preparedness and responsiveness. Any company's approach to cyber-security should be aligned with business goals and priorities, and should consider both current and emerging business practices and technology trends.

Contributed by: **Alex van der Wolk**
Partner, Morrison & Foerster LLP (Lex Mundi member firm for USA, California)

Let China and Europe Fight It Out Over Data-Privacy Rights

The Wall Street Journal
April 5, 2017

The Trump administration and US tech companies are confronting major trade barriers in Europe and China. The problem in both cases is consumers' right to privacy.

China is fostering national champions that are friendlier to state surveillance than Silicon Valley firms. Meanwhile, Europe is threatening to punish American companies because US surveillance policy doesn't meet its data-protection standards.

The solution is simple: Step back and let America's two biggest trade adversaries fight it out.

China's hostility to US tech companies became clear when Google found itself frozen out of the world's biggest search market. Since then, China has systematically squeezed US internet companies and favored local copycats. Now grown fat in a protected market, many of those local champions are preparing to challenge Silicon Valley for global dominance. That's problem No. 1.

Problem No. 2 is Europe's determination to impose its privacy law on the US. The European Union restricts the exportation of personal data to countries whose data-protection policies aren't "adequate" by EU standards.

Perhaps Freud's "narcissism of small differences" explains Europe's 20-year history of threatening to cut off data flows to the US. Or maybe it's the leg-up the policy gives to Europe's dwindling tech industry. But there's no doubt that Europe loves the fight. The EU will soon arm its privacy enforcers with the authority to impose data-protection fines on American tech companies. These could run as high as 4% of global revenue. For Google, that's close to $4 billion.

This massive leverage is increasingly being used not to regulate the use of personal data in advertising or the private sector but to attack US counterterrorism tools. In a recent lawsuit brought by the Austrian student Max Schrems, the European Court of Justice objected to the way US authorities use data to find terrorists.

Relying on a garbled version of the Snowden leaks, the court declared that US law doesn't adequately protect privacy in the fight against terrorism. Now the EU is threatening to punish US companies with $4 billion fines if the Trump administration rewrites the Obama administration's limits on intelligence collection.

Instead of rushing to propitiate EU negotiators, Donald Trump's team should try a different approach. Introduce them to Xi Jinping, who makes no bones about using data to keep the Chinese people in line. Before imposing sanctions on US companies over America's human rights practices, maybe the EU ought to investigate China's practices.

There should be plenty of data exports to investigate. China's autarchic policies have made its champions strong in every part of the wireless internet, from back-end switches to consumer phones. In the app economy, WeChat boasts more than 800 million active users and is aggressively penetrating the European market. The Chinese company Wish is one of the top three online-shopping apps in the UK and is outpacing Amazon in France.

WeChat recently bragged in Brussels about how much data it collected on potential European tourists, and how seamlessly it could move around: "WeChat allows merchants to target a well-defined audience, based on age, gender, purchasing power, geographical location, likelihood to visit a country soon, etc., attract them as followers and send them personal communication messages, special promotions or coupons both in China and once they are travelling."

If they're traveling in Europe, those tourists are protected by the same European privacy law that has bedeviled the US for 20 years. So if it's sauce for the American goose, why not for the Chinese gander? Hard-nosed Trump-administration negotiators should certainly be asking that question. Because "arbitrary or unjustifiable discrimination" in administering Europe's data protectionism is a violation of international trade law.

But why wait for the negotiators? As Mr. Schrems has shown, anyone whose data has been exported to another country can challenge the adequacy of that country's law. So should you find yourself in Europe, if only for an extended visit, just open your phone, download WeChat, and subscribe. That's enough to make you a plaintiff – and shake the world.

Why? Because that lawsuit will force both Europe and China to make hard choices. How much diplomatic and economic pain is Europe prepared to suffer in support of its privacy *mission civilisatrice*? Will China defend its surveillance regime at the risk of exposing its tech giants to $4 billion in fines?

For Americans, this conflict would be a chance to break out the popcorn. But it could also resolve a contradiction that has bedeviled the tech industry for a generation. Because if Mr. Xi forces Europe to put limits on its data-protection imperialism, the EU will have to make the same concessions to the US.

Contributed by: **Stewart Baker**
Partner, Steptoe & Johnson LLP (Lex Mundi member firm for USA, District of Columbia)

First Steps in a Cyber-Breach

1. Contain the Breach.

Once a cyber-breach has been detected, the breach must be contained to mitigate the damage and prevent further unauthorized access to or use of personal identifiable information. Ideally, all system and audit logs and evidence will be preserved in the process.

2. Conduct an Initial Analysis of the Breach.

At the same time, the organization must gather details about the breach and assess what information was exposed and who was impacted. While some organizations choose to conduct an investigation in house, many choose to hire an outside vendor specializing in digital forensics, often under lawyer-client privilege.

3. Comply with Applicable Data Breach Notification Requirements.

A number of countries have laws requiring organizations to notify individuals and/or the government following a data breach. California was the first jurisdiction to enact a broad data breach notification requirement. Most U.S. states and territories now have data breach notification statutes, which typically apply broadly to organizations that acquire, own, or license computerized data including personal identifiable information of individuals who reside within that jurisdiction. Certain U.S. federal statutes also apply to certain types of organizations and protected information (e.g. the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the American Recovery and Reinvestment Act).

These statutes generally require notification to individuals whose personal identifiable information has been or may have been compromised. They may also require the government be notified, and certain statutes require notification to credit reporting agencies. Typically, notification must be made without "unreasonable" delay, but certain statutes require more prompt notification (for example, California requires notification to individuals within 5 days of detection of a breach for protected medical information). These statutes normally specify the appropriate method of notification, and some statutes describe the content required. If the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation.

A number of individual European countries currently have data breach notification laws (including the Netherlands, which passed a law in January 2016 requiring data controllers to notify the Data Protection Authority of data security breaches). In addition, the European Commission's ePrivacy Directive established breach reporting obligations for telecommunications service providers, and the General Data Protection Regulation (GDPR) – which becomes effective May 25, 2018 – will extend data breach notification requirements to all organizations (including a requirement to notify the relevant supervisory authority within 72 hours). Canada and Australia have also recently enacted data breach notification laws, but like the GDPR, they have not yet entered into force.

4. Comply with Other Legal Obligations.

For example, certain U.S. states require covered entities to offer credit monitoring services free of charge for one year to consumers whose personal identifiable information has been exposed in a data breach.

5. Bring in Your Communications People.

In coordination with the legal response, an organization should carefully consider its public relations response and adopt a press strategy that focuses on providing accurate information quickly.

6. Conduct More Intensive Forensic Analysis.

After an initial analysis of the breach, it will be necessary to fully understand the circumstances of the breach to explain what happened and prevent future incidents. If the organization already has an incident response plan in place, it should be followed (and modified as necessary – no plan survives contact with reality).

7. Prepare to Defend Against Lawsuits.

Retain outside legal counsel, if necessary, to defend against lawsuits brought by either government or individuals.

Contributed by:
Stewart Baker, Partner
Claire Blakey, Associate
Steptoe & Johnson LLP (Lex Mundi member firm for USA, District of Columbia)

Acknowledgments

Lex Mundi wishes to thank the following:

Stewart A. Baker, Former Assistant Secretary for Policy at the U.S. Department of Homeland Security, and Partner, Steptoe & Johnson LLP (member firm for USA, District of Columbia)

Freddy Dezeure, Head of CERT-EU, CERT-EU

Helen Graham, Chief Privacy Officer, Shell

George Little, Former Assistant to the U.S. Secretary of Defense for Public Affairs and Pentagon Press Secretary, Former Director of Public Affairs and Chief of Media Relations for the CIA, and Partner, Brunswick Group LLC

Alex van der Wolk, Partner, Morrison & Foerster LLP (member firm for USA, California)

Steven E. Zipperstein, Chief Legal Officer, Blackberry Ltd.

Participating Lex Mundi member firms:

Arendt & Medernach SA (member firm for Luxembourg)
Chiomenti (member firm for Italy)
Demarest Advogados (member firm for Brazil)
Egorov Puginsky Afanasiev & Partners (member firm for Ukraine and Russia)
Faegre Baker Daniels LLP (member firm for USA, Indiana and USA, Minnesota)
Gide Loyrette Nouel A.A.R.P.I. (member firm for France)
Houthoff (member firm for Netherlands)
Jenner & Block LLP (member firm for USA, Illinois)
Liedekerke Wolters Waelbroeck Kirkpatrick (member firm for Belgium)
Marval, O'Farrell & Mairal (member firm for Argentina)
Morrison & Foerster LLP (member firm for USA, California)
Noerr LLP (member firm for Germany)
Pestalozzi (member firm for Switzerland)
Shardul Amarchand Mangaldas & Co. (member firm for India)
Steptoe & Johnson LLP (member firm for USA, District of Columbia)
Uría Menéndez (member firm for Spain)

Participating corporate counsel:

Aggreko Plc
Air France
Banco Santander, S.A.
Cablevisión
Ivan Lorenzo
Cargolux
Cosan
Diageo
The Edrington Group Limited
FerroAtlántica
Fibria Celulose SA
Hunter Boot Limited
John Wood Group
Johnson Controls
Katoen Natie International
Khazanah Europe Investment Limited
Magneti Marelli S.p.A.
Novartis Pharma AG
Philips
Pirelli & C. S.p.A.
Siemens Gamesa
Société Générale
Tata Global Beverages
Total

About Lex Mundi

Lex Mundi is the world's leading network of independent law firms with in-depth experience in 100+ countries.

Lex Mundi member firms offer clients preferred access to more than 21,000 lawyers worldwide – a global resource of unmatched breadth and depth. Each member firm is selected on the basis of its leadership in – and continued commitment to – its local market. The Lex Mundi principle is one independent firm for each jurisdiction. Firms must maintain their level of excellence to retain membership within Lex Mundi.

Through close collaboration, information-sharing, training and inter-firm initiatives, the Lex Mundi network is an assurance of connected, on-the-ground expertise in every market in which a client needs to operate. Working together, Lex Mundi member firms are able to seamlessly handle their clients' most challenging cross-border transactions and disputes.

Lex Mundi member firms are located throughout Europe, the Middle East, Africa, Asia and the Pacific, Latin America and the Caribbean, and North America. Through our nonprofit affiliate, the Lex Mundi Pro Bono Foundation, members also provide pro bono legal assistance to social entrepreneurs around the globe.

Lex Mundi
The World's Leading Network of Independent Law Firms
2100 West Loop South, Suite 1000
Houston, Texas USA 77027
1.713.626.9393
www.lexmundi.com

Lex Mundi
World Ready

Lex Mundi Global Cyber-Breach Resources
Complimentary Access: **www.lexmundi.com/Cyber-Security**