Recognizing and Mitigating Cyber Security Risks in the Design and Construction Industry
Recognizing and Mitigating Cyber Security Risks in the
Design and Construction Industry

The U. S. Department of Homeland Security and Department of Energy define cyber security risk as:

risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information, IT [Information Technology] and/or OT [Operations Technology]. Cyber security risk is one component of the overall business risk environment and feeds into an organization’s enterprise risk management strategy and program. Cyber security risk cannot be completely eliminated, but it can be managed through informed decision-making processes.

While all businesses face cybersecurity risks, the design and construction industries are confronted with heightened risk due to the ever-increasing use of computer technology and linked devices. The volume of stored data and points of access to that data render design and construction firms rich targets for incursion. So too, the inherent fluidity of the construction labor force is viewed as a unique security risk. For each employee in the labor force, there is a wealth of data which the employer must safeguard, and for each employee utilizing the employer’s digital technology, there is opportunity for data breach.

While the massive data breach incurred by Target was eye opening front-page news, the less known detail is that the password stealing bot program through which the breach was perpetrated was apparently initiated via a malware-laced email phishing attack sent to employees of Target’s HVAC contractor. Other recent construction industry data incursions have been reported by design firms and contractors. Trends
also suggest that building management systems may become increasingly targeted as those systems continue to evolve and become more fully integrated. The emerging Internet of Things (IOT), involving interconnectivity of devices and hardware to the internet, including “smart hardware” within the built environment, such as elevators, door locks, thermostats, and lighting systems, for remote control presents unique cyber security challenges. Only through a culture of awareness and vigilance, together with carefully defined breach response plans, and effective insurance coverage for the cost of response and potential losses can firms successfully mitigate cyber security risks.

I. The Data Breach Landscape

Current Data Breach Trends

The duty to protect information that is collected, stored and used by companies has been most often associated with personally identifiable information (PII), personal health information (PHI), and personal financial information (PFI). In its annual Data Breach QuickView Report for 2017, cyber security firm Risk Based Security reported that there were 5,207 breaches reported through the end of 2017, exposing approximately 7.89 billion records. Over 2016, the number of reported breaches was up 24.1%, and the number of exposed records was up 24.3%.

The five largest breaches of 2017 exposed approximately 5.7 billion records or 72.2% of all records exposed. The Business sector accounted for 39.4% of reported breaches, followed by Medical (8.1%), Government (7.2%), and Education (5.3%). Data
leaks from organizations that could not be identified accounted for 40% of confirmed breaches.

The Business sector accounted for 83.9% of the total records exposed, followed by Unknown (12.3%) and Government (3.7%). Medical and Education sectors combined continue to account for less than 1% of the total records exposed this year (2017). When compared to the above, it is clear that, while the source of the data cannot always be confirmed, the overwhelming volume of data compromised originates from the general Business sector.

Following prior quarters’ trends, Web (inadvertent online disclosure) was the leading cause of records compromised in 2017, accounting for 68.7% of exposed records, but only 5% of reported breaches. The leading cause of breaches for the year was Hacking (unauthorized intrusion), accounting for 55.8% of incidents. The percentage of records exposed due to Hacking was 29.8%, or 2.3 billion records. The number of breaches in 2017 confirmed to have exposed one million or more records was 89, bringing the 10-year total for such “mega” breaches to 344. 2017 finished with eight breaches on the Top 20 List of All Time Largest Breaches.

In the first quarter of 2018, 686 breaches were been reported through March 31st, exposing approximately 1.4 billion records. Compared to Q1 2017, the number of reported breaches is down from 1,442 incidents and the number of exposed records is down from 3.4 billion. The number of disclosed instances of phishing for employee W-2 data dropped from 214 in Q1 2017 to 31 in Q1 2018.

The Business sector accounted for 50.4% of reported breaches, followed by
Government (14.4%), Medical (10.2%), and Education (7%). One incident in India accounted for approximately 81% of the records exposed in Q1 2018. Setting aside the quarter’s one “mega breach”, the Business sector accounted for 97.9% of the records exposed followed by Government at 1.1%. As in 2017, the Medical and Education sectors combined accounted for less than 1% of the total records exposed in the quarter.

Fraud captured the top spot for the breach type compromising the most records, accounting for 1.27 billion exposed records during the quarter. However, fraud came in as only the seventh most common breach type, accounting for 4.8% of reported breaches. The leading cause of breaches for the quarter was hacking (unauthorized intrusion), accounting for 38.9% of incidents. The percentage of records exposed due to Hacking was 10.9%, or 159 million records.

Common Schemes and Types of Incursion

**Hacking**: Hacking simply refers to the unauthorized access to digital information within a computer or a network, and can be perpetrated by a number of the various schemes described below.

**Malware, Viruses and Worms**: Malware refers to malicious software that is designed to cause damage to a stand-alone computer or a network of computers. A virus is a program written to enter a computer and damage, alter or corrupt files or data. Most viruses have the capacity to replicate themselves. Worms are programs that typically copy themselves again and again on a local drive or network shares. Through replication, worms can exploit vulnerabilities in operating systems.
**Phishing and Spearphishing:** These are among the most prevalent forms of attack. Using emails designed to trick users into compromising systems and data, the “phisher” seeks to compromise systems to obtain usernames, passwords, and other account and/or financial data. Phishing emails appear to be from a known or trustworthy sender, such as a customer or bank, or even a government agency. Spearphishing is simply a targeted form of phishing, where the malicious attack is directed to a specifically targeted recipient.

**Ransomware:** Ransomware is malware that encrypts files, rendering them inaccessible, and requiring the victim to pay a “ransom” to unlock the data.

**Social Engineering – Baiting, Scareware:** Refers to techniques for tricking users into sharing sensitive data. Through baiting, online ads might lead to malicious sites or encourage users to download a malware-infected application. Scareware bombards the victim with false alarms and fictitious threats. Users are deceived into thinking their system is infected with malware, prompting them to install software that has no real benefit.

**Point-of-Sale (POS) intrusions:** The POS device is compromised by installing malware to collect magnetic stripe data in process, and retrieving data for financial gain.

**Web Application Attacks:** Web application attacks target code-level vulnerabilities in the application, and impair authentication mechanisms. The utility and manufacturing operations are common targets.
Personally identifiable information (PII), payment card information (PCI) and personal health information (PHI) remain at the top of targeted data sought and exposed by data incursions. Data breaches exposing PII represented 36% of the claims in the dataset; PCI, 16%; and PHI, 15%. Non-card financial information was exposed in 5% of the claims. Compared to a 2016 study, there was a higher number of cases reported in 2017 relating to the theft of Trade Secrets or Intellectual Property / Trademark Infringement.

The range of potential impacts from a successful cyber-attack is wide and varied. First Party losses may include data loss and restoration expenses, notification costs and credit monitoring services, IT/forensic services and expenses, lost income, productivity, business interruption expenses, crisis management and public relations expenses, and criminal extortion, theft, and fraudulent transfers. Third Party losses arising out of a data breach can include privacy and network liability, regulatory liability, media liability, and technology errors and omissions. In its 2016 annual review of the costs of cyber-crime, the Ponemon Institute found that the single largest cost impact from cyber-crime is information loss (an average of 39 percent), followed by business disruption at 36 percent. The study further revealed the time it takes to resolve the consequences of the attack increases the cost of a cyber-crime. Detection and recovery activities accounted for more than fifty-five percent of total internal response costs in 2016, followed by containment and investigation costs at eighteen and thirteen percent, respectively.

II. Data Breach Reporting Requirements
A multitude of state and federal reporting requirements have been instituted, and require prompt disclosure of data breach incidents by both private businesses and government contractors.

**State Law Requirements**

No business – large or small – is safe from attack. In 2017, Equifax – a consumer credit reporting agency – was breached by hackers, exposing 143 million people to the potential of identity theft. On the other end of the spectrum, in 2016, half of all small businesses were breached by hackers.

In response to these breaches, all 50 states and the District of Columbia have passed laws mandating that businesses must notify affected individuals when their information has been compromised. These reporting requirements may cover residents only or all affected individuals. Businesses may also be required to notify regulatory agencies, the state attorney general, or consumer credit reporting agencies in the event of a breach, and these requirements may be triggered by the number of individuals affected by the breach. While most states only require that these notifications happen as expediently as possible and without unreasonable delay, some states require that the notifications happen within a set number of days after the breach is discovered.

The following states require businesses to notify all affected individuals, regardless of whether the individuals are residents of the state: Alabama, Arizona, Hawaii, Iowa, Mississippi, New Hampshire, North Carolina, Oregon, Texas, Vermont, and Wisconsin. The rest of the states and the District of Columbia require businesses to notify only those affected individuals who are residents of that state.
The vast majority of states only require notifications to be given as expeditiously as possible or without any unreasonable delay. The exceptions to this rule are Connecticut (90 days); Delaware (60 days); Florida (30 days); New Mexico (45 days); Ohio (45 days); Rhode Island (45 days); South Dakota (60 days); Vermont (45 days); Washington (45 days); and Wisconsin (45 days).

Certain states require disclosure to additional entities regardless of the number of individuals affected by the breach: Maine (the appropriate state regulators within the Department of Professional and Financial Regulations or, if the entity is not regulated, the Attorney General); Montana (copy of notice sent simultaneously to Attorney General’s Office); New Hampshire (regulator with primary regulatory authority or the Attorney General’s Office); New Jersey (notification to Division of State Police in the Department of Law and Public Safety prior to disclosure to consumer); Oregon (Attorney General); South Dakota (all nationwide consumer reporting agencies); Vermont (Attorney General or Department of Financial Regulation within fourteen days); and Virginia (Attorney General).

Other states require entities to make these additional disclosures if the number of individuals affected exceeds a certain threshold. States commonly require all nationwide credit reporting agencies to be notified in the event of a significant breach. Additionally, some states require additional agencies be notified of the breach if a certain number of individuals are affected.

**Disclosure Requirements for Federal Contractors**

The threat of data breaches is not confined to private enterprise. Indeed, an even
greater target is the United States government and the private companies who perform contracts for it, as a data breach in these entities can expose sensitive government information as well as citizens’ personal identification information. As of 2018, 70% of federal agencies have been breached, and 57% have been breached in the past year. Because of this threat, federal agencies have implemented cybersecurity and disclosure requirements in an attempt to stop breaches and minimize their harm.

It is impossible to provide an all-encompassing overview of the disclosure requirements for federal contractors, as these requirements will be both contract-specific and agency-specific. Even so, the Office of Management and Budget has set out a general policy that Federal agencies should abide by in preparing to respond to a data breach. Additionally, general requirements from a sampling of three agencies – the Department of Justice (“DOJ”); the Department of Defense (“DOD”); and the General Services Administration (“GSA”) – are presented below.

In 2014, Congress passed an updated version of the Federal Information Security Modernization Act (“FISMA”). The purpose of FISMA is to establish oversight and accountability for federal agencies in the area of data security and data breach reporting. As part of that oversight, the Office of Management and Budget created a uniform breach notification policy and guidelines for all federal agencies (the “Breach Policy”).

Under the Breach Policy, agencies are to include certain terms in every contract that will enable the agency to address a data breach involving a contractor. These terms include a requirement that contractors “cooperate with and exchange information with
agency officials . . . in order to effectively report and manage a suspected or confirmed breach” and that contractors must “report a suspected or confirmed breach . . . as soon as possible and without unreasonable delay.”

The Breach Policy allows, but does not mandate, the agencies to require contractors “to notify any individuals potentially affected by the breach.” Individual agencies can also decide whether they will require contractors to “take countermeasures to mitigate the risk of harm to potentially affected individuals.” Additionally, if the contractor will be providing notification on behalf of the federal agency, “such activities shall be in accordance with OMB guidance and the agency’s breach response plan and shall be coordinated with and subject to prior written approval by the head of the agency.”

Response requirements vary between agencies and according to the terms of the contract involved. For example, the DOD requires contractors who discover a cyber incident to report the incident to them within 72 hours. The GSA requires all suspected or confirmed breaches to be reported to GSA Office of the Chief Information Security within one hour of the discovery of the event. The DOJ requires all suspected or confirmed breaches to be reported to DOJCERT within one hour of discovery; additionally, contractors are also required to notify the Contracting Officer and the Contracting Officer’s Representative within one hour of discovery.

III. The General Data Protection Regulation – Looming International
Considerations

What is the GDPR

The EU’s General Data Protection Regulation (Regulation (EU) 2016/679) updates long-standing privacy laws to reflect the modern world. After a multi-year legislative process, the GDPR was born. It took effect on May 25, 2018, and represents a seismic shift in data protection requirements. While the GDPR is a regulation applicable in the EU, the GDPR’s reach extends well beyond the EU.

Does it Apply to You

Unlike privacy laws in the U.S. and Canada, EU data protection law is comprehensive rather than sector-specific. However large or small the business, in whichever sector it may operate, if a business controls or processes personal data then it’s likely in scope. The GDPR has very broad scope. In fact, it has an extra-territorial reach that can come as a shock to many non-EU businesses. One of the GDPR’s main goals is to protect the personal data of individuals in the EU wherever that data may be located.

With limited exceptions, the GDPR applies to any person who processes personal data about an individual in the EU. Processing in this case refers to collecting, storing, using, disclosing, or otherwise performing operations on personal data. It’s a broad definition and concept. Personal data is equally broad. It refers to any information relating to an identified or identifiable natural person (which are called data subjects). An identifiable natural person is one who can be identified, directly or indirectly, in
particular by reference to an identifier such as a name, an identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

**Territorial scope**

The GDPR applies directly to businesses established in the EU and businesses who reach out to individuals in the EU for business purposes. The intent is to protect people in the EU wherever their data may be – it’s about enforceability.

In practice, this means that if your business is headquartered or has a subsidiary or other establishment in the EU, then the GDPR will apply. Further, even if your business does not have an EU establishment but it monitors the behavior of or otherwise offers good or services to individuals in the EU, then the GDPR will apply.

According to guidance, merely having a non-EU website that someone in the EU happens to order something from isn’t enough to bring a business in scope for the GDPR. However, if that same website were to have a German language version that accepted payment in Euros and otherwise reasonably sought business from German citizens, then the GDPR would likely apply.

As of the time of this writing there is no clear rule or guidance suggesting that pure business-to-business arrangements bring a business in scope for the GDPR. In terms of territorial scope, the GDPR’s focus seems to be on protecting individuals as individuals and/or consumers rather than individuals in their capacity as business representatives. It remains, however, an open and often-discussed topic. If, however,
**territorial** scope does apply, then under the GDPR’s *material* scope, the personal data of individuals in their capacities as business representatives must still be protected as personal data.

**Notice and Transparency**

Article 5(1) of the GDPR states simply that personal data must be processed “lawfully, fairly, and in a transparent manner in relation to the data subject.” Recital 39 explains:

It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.

**Privacy by Design**

Privacy by design means that data protection should be considered from the beginning of each project. How much data is required, how must it be used, how long can it be retained, how can it be secured.

Article 25 provides details on how businesses should implement privacy by design. For example, it states that businesses should “both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as
pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of [the GDPR] and protect the rights of data subjects.”

Minimum and Proportional

Basically, this means if you don’t need it then don’t use it. Article 5(1) requires that personal data be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.” It’s a simple concept with many vectors: what data elements are necessary, for which purposes, accessible by whom, for how long? Those considerations and others all play a role. The key is being continually vigilant that you’re limiting the processing of personal data to what’s actually necessary, as opposed to what’s simply easy or convenient.

Key Requirements

While this is by no means a comprehensive list, among the GDPR’s most prominent requirements (along with some of the Articles describing them) are to:

**Ensure a Lawful Basis for Processing (Articles 5-6):** This can take many forms, including most commonly, consent of the data subject and legitimate interests of the controller. Consent is harder to establish under the GDPR than under prior laws. Article 4 defines consent to mean “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him
or her.”

**Ensure a Lawful / Adequate Mechanism for Transferring Data out of the EU (Articles 44-50):** This, too, can take many forms. The most common would be Binding Corporate Rules, Standard Contract Clause agreements, and (for transfers to the U.S.) certification under the EU-U.S. Privacy Shield framework. The GDPR also introduces new lawful transfer mechanisms such as certain approved codes of conduct.

**Evaluate and Respond Timely to Data Subject Rights (Articles 12-23):** The GDPR greatly expands the rights of data subjects. With respect to their personal data, data subjects now have the right to request access, rectification, erasure, restricted processing, portability, and more. Businesses must respond to data subject rights requests without undue delay and in any event within one month of receiving the request, though it is possible to obtain an extension of up to two additional months under certain conditions. Businesses can have interests in the personal data, too, so responding to such rights requests often involves a balancing test.

**In Many Cases, Hire a Data Protection Officer (Articles 37-39):** Data Protection Officers are required for some companies and recommended for others. DPOs are appointed based in part on expert knowledge of data protection laws. They serve as independent, lead advisors on data protection issues and must report to the highest management level. The GDPR sets forth many roles and parameters for DPOs, including that of ensuring employees receive proper awareness and training.

**Implement Appropriate Technological and Organizational Security Controls (Article 32 and more):** This is a flexible, scalable requirement. The GDPR intends for
businesses to tailor their security controls to their unique data and environments by, for example, taking into account “the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.” Four things are mentioned as controls for businesses to consider, though the GDPR does not intend this as an exhaustive list: (1) the pseudonymization and encryption of personal data; (2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

**Breach notification to DPAs and data subjects (Articles 33-34):** A breach must be reported to the supervisory authority within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to the rights and freedoms of an individual. The breach must also be reported to affected data subjects if it is likely to result in a high risk to them.

**Potential penalties:** The GDPR has a tiered and quite substantial penalty structure. Lower-risk violations can be penalized up to the greater of 2% of global annual revenues or $10MM Euros, and higher-risk violations can be penalized up to the greater of 4% of global annual revenues or $20MM Euros. Examples of lower-risk violations include the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39, and 42 to 43. In addition to these penalties, any person who has suffered damage from GDPR violations has a right to compensation under Article 82.
IV. Mitigation of Risk – Incident Response Capability and Incident Response Plan

As the range of data breach vulnerabilities and experience with data breach incidents continues to evolve, development of an incident response capability and a detailed incident response plan – a roadmap for incident handling – has become the cornerstone of risk mitigation. Developing the capability to respond and the plan by which that capability is executed involves key management and IT and IS personnel, and increasingly, may also include the participation of data security consultants and insurers who have developed critical resources for breach avoidance and mitigation. An effective plan enables detection of an attack, and establishes procedures to minimize or contain the damage.

Establishing a response capability should include the following actions: (1) creating an incident response policy and plan; (2) developing procedures for performing incident handling and reporting; (3) setting guidelines for communicating with outside parties regarding incidents; (4) selecting a team structure and staffing model; (5) establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies); (6) determining what services the incident response team should provide; and (7) staffing and training the incident response team.

A well-planned response capability enables consistent and timely incident
handling methodology so that the appropriate actions are taken to minimize loss or theft of information and disruption of operations. The response plan further enables the use of information gained during the incident to enhance system protections and contend with potential legal issues. The NIST recommends an incident response plan include the following elements: (1) mission; (2) strategies and goals; (3) senior management approval; (4) organizational approach to incident response; (5) how the incident response team will communicate with the rest of the organization and with other organizations; (5) metrics for measuring the incident response capability and its effectiveness; (6) roadmap for maturing the incident response capability; and (7) how the program fits into the overall organization.

A breach incident will quite probably trigger the need to communicate with outside parties, including internet service providers (ISPs), the vendor of vulnerable software, clients or customers, law enforcement, and the media inquiries. The incident response plan should establish policies and procedures regarding information sharing, and should document all contacts and communications with outside parties. Media communications are best managed by a single point of contact within the company. Before information is disclosed to third parties, the company should carefully evaluate the need to obtain a nondisclosure agreement to protect the confidentiality of protected or sensitive information.

Depending on the size and resources of the company, the incident response team may consist of only employees who are supported only by limited outside technical support. For many companies, the predominant practice is to outsource 24-hours-a-day, 7-days-a-week (24/7) monitoring of firewalls and other security devices to
an offsite managed security services provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the company’s incident response team. When using an MSSP or other outside security vendor, the company must ensure the vendor is apprised of what incidents are of the greatest threat to operations, which resources are critical, and what the level of response should be under various sets of circumstances. The company should also report all changes and updates made to its IT infrastructure, network configuration, and systems.

The response plan should identify predetermined strategies and procedures for containing the incident (e.g., shut down a system, disconnect it from a network, disable certain functions). The company should develop separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making.

V. Data Privacy Coverage and the Claims Process – the Insurer’s Perspective

Data Privacy Insurance

Aside from stand-alone cyber/privacy policies, insurance coverage for a data/privacy breach claim may lie within a number of types of policies, including commercial general liability, management liability, D&O liability, E&O and professional liability, commercial crime, blended products, and public entity. Such coverage is commonly subject to sub-limited endorsements. Sub-limits for crisis management expenses, notification costs and regulatory investigations are common, but many
carriers are willing to negotiate the size of the sub-limit, and often with no increase in premium.

Stand-alone insurance coverage is now widely available for four general categories of potential exposure: liability of the insured arising out of failure to properly secure private data; incident response costs following a data breach, including investigation, public relations, customer notification, and credit monitoring; forensic services and card reissuance costs in the event of a payment/credit related breach; and some potential limited coverage for defense costs incurred investigating and defending exposure to regulatory penalties, including the cost to investigate, defend, and settle such penalties.

A 2017 insurance market survey identified six principal considerations in the procurement of cyber/privacy insurance: (1) types of coverage and limits available; (2) coverage provided; (3) coverage triggers; (4) types of data covered; (5) remediation costs covered; and (6) remediation coverage services.

Data privacy/cyber insurance generally distinguishes between two broad loss categories, first party and third party. First-party losses relate to those directly suffered by the insured (i.e. the “first” party to the insurance contract), while third-party liability relates to claims brought by parties external to the contract (i.e. the “third” party) who suffer a loss allegedly due to the insured’s conduct. First-Party coverage extends to four principal categories of risk:

**Crisis Management & Identity Theft Response:** Includes the cost to notify affected customers, providing credit monitoring services, conducting forensic
investigations, and for expenses incurred in retaining a crisis management or public relations firm for the purpose of protecting/ restoring the company’s reputation.

**Cyber Extortion:** Provides coverage to pay ransom or investigate a threat to destroy, steal or use confidential information; introduce malicious code into a computer system; corrupt, damage or destroy a computer system; or restrict or hinder access to a computer system.

**Data Asset Protection:** Covers costs incurred to restore, recreate or regain access to any software or electronic data from back-ups or from originals or to gather, assemble and recreate such software or electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage.

**Network Business Interruption:** Reimbursement for loss of income and/or extra expenses resulting from an interruption or suspension of systems.

Third-Party Coverage extends to two principal categories of risk:

**Network Security Liability:** provides coverage for third-party claims arising from a breach in network security or transmission of malware/viruses to third-party computers and systems.

**Privacy Liability:** Covers third-party claims for failure to properly handle, manage, store or otherwise protect personally identifiable information, confidential corporate information and unintentional violation of privacy regulations.
It is important to understand the triggers of coverage under any policy affording coverage. Some policies are triggered on the date the loss occurs, while others are triggered on the date that a claim is made against the insured. In order to provide proper notice, you need to understand how coverage applies under each policy you purchase. Companies should also consider whether to require their own third-party vendors to obtain cyber insurance coverage, and if so, to insist those policies cover any liability to the company resulting from a breach affecting the third-party vendors, including by adding the company as an additional insured. Policies should be carefully reviewed for any insured v. insured exclusion, and if possible, such endorsements should be eliminated, as the exclusion that might remove coverage for any third-party vendor claim. The company should also carefully coordinate any contractual indemnity terms within its business.

Claims Handling Process

The typical life cycle of a data breach claim involves four distinct phases: (1) discovery of the breach; (2) investigation (forensic and legal analysis); (3) response (notification, credit monitoring, public relations); and (4) defense (possible class actions, income loss, fines penalties, reputational loss). By its nature, a data breach incident can quickly trigger substantial costs stemming from response measures incurred on many potential fronts. In the case of a computer system breach, there is the need to forensically deduce the nature and extent of what has occurred, and to eradicate the damage and shore up the system. There will most probably be state reporting requirements, and potential public relations issues. For the insured and its insurer, the earliest reporting of an incident and the rapid deployment of response resources is
critical to mitigating damages that can ensue. As a consequence of these inherent time sensitive factors in a data breach setting, and of an expanding claim handling experiences, most insurers have developed robust claims handling procedures for cyber claims that involve rapid deployment of response measures.

Similar to other types of “rapid response” claims teams, the experienced insurer has already established relationships with skilled legal counsel, IT forensics experts, public relations specialists, and credit monitoring providers. Insurers adept in the cyber claims handling process have developed extensive experience in deploying highly skilled and pre-approved vendors in each of these disciplines, and many policies require insureds to select vendors from a pre-approved list. Some insurers engage third-party incident managers to coordinate the incident response and devise and manage the action plan to get the business back on track. Since time is critical, these ready resources ensure that the breach response is not needlessly delayed. Establishing a central point of contact within the company is essential to the response management process.

The elements and timeline of initial claims communication are typically more aggressive and regimented, and might include: (1) one hour call-back from incident manager; (2) three hour call-back from IT forensics (as required); (3) eight-hour update conference with key suppliers; and (4) 48-hour update with agreement of a clear incident management plan

The forensic investigation is generally organized around identifying and eradicating any intrusion, and thereafter treating its consequences. In coordination with
the insured, the insurer will solicit a forensic investigation proposal. The near-term objective is to stem the technical problem (e.g. enhanced firewalling), and the long-term objective is to sort out and rectify the consequences of the intrusion.

Enabling an effective and timely response may require the flow of significant volumes of company information, both with respect to the computing systems involved and the identity of customers or clients whose data has been exposed. The company may be required to submit an incident report setting forth detail about the breach. Notification forms seek information regarding the general nature of the breach, the expanse of affected third-parties and potential economic losses (severe, moderate, low), and the method by which breach occurred, e.g. unauthorized password access. Certain types of very detailed information may also be sought, including details of operating systems, the identity of effected network devices, IP addresses and server information.

Regardless of the insurer's claims handling expertise, the company's first line of defense remains its own level of breach response preparedness. Attempting to create a breach response capability or breach response plan at the time of a claim would be akin to recharging the fire extinguisher at the outbreak of a fire – no meaningful protection is attained. If a breach arises, the insurer will work with the insured, counsel, and consultants to identify elements of the response plan that may require priority, as well as necessary additional action items.