Comments on Developing a Framework to Improve Critical Infrastructure Cybersecurity

Response to RFI

Gemini Security Solutions

April 8, 2013

Table of Contents

1 Background

Gemini Security Solutions, Inc specializes in assisting companies in determining their business critical information and then helping those companies determine the best way to protect that data. We work with large companies and small companies - primarily in the healthcare industry. We help companies determine their risks and exposure to risk from sharing that critical information with business partners. As part of that work, we have assessed over 500 companies in multiple industries, very large companies, very small companies, highly regulated, and not regulated at all. We have seen and evaluated these companies' capabilities in information security and believe that our experiences can provide valuable input to this RFI.

1.1 About Gemini Security Solutions

Gemini's team of builders, breakers, and tinkerers brings a rich tapestry of experience through a diversity of skills, backgrounds, and passions. We serve as trusted advisors, providing expert assistance to those tasked with protecting some of the most valuable intellectual property in the world.

Our independent and impartial team moves at the speed of small business, but has big business experience. Our core customers are heavily regulated Fortune 500 organizations. By discovering critical patterns and illuminating their blind spots, our clients count on us to take the risk out of reducing risk.

geminisecurity.com
4451 Brookfield Corporate Dr.
Suite 200
Chantilly, VA 20151
info@geminisecurity.com

2 Current Risk Management Practices

In addition to the questions asked by the RFI below, we also believe that an important question to ask and for the Framework to help answer is: "what exactly *is* critical infrastructure?" There are the obvious ones that can be assumed and have been explicitly pointed out by government agencies such as electricity, water, etc. Are other companies and industries also critical infrastructure? Is the ability to manufacture consumer products (soap, acetaminophen, ibuprofen, etc.) a critical capability? What about the research and

quality departments of pharmaceutical companies? There is a strong argument for hospitals and doctors, and even pharmaceutical manufacturing to be part of critical infrastructure, but just because one part of a company is deemed critical, does that mean that all other parts are as well - just because they share an IT infrastructure?

Defining or assisting companies in defining what should be critical infrastructure should be one of the many focuses of the Framework. **What exactly should we be protecting?** In some case, especially smaller companies, it may not be obvious unless a customer tells them that they are dependent on the company's services or product.

2.1 What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

There are many challenges in improving cybersecurity practices across critical infrastructure.

Businesses generally see IT - and cybersecurity - as a cost center, which increases the overhead of business operations. In the highly regulated industries such as healthcare, pharmaceuticals, and financial services, cybersecurity is taken into account only so much as it protects the business from fines and fees. There are some businesses (generally on the smaller side) where the company owners actually care about the security of the information they are the custodians of.

Many, especially small, companies also lack sufficient knowledge to begin to contemplate cybersecurity risk management. They have enough on their plate coping with business risks. These small companies generally take their cybersecurity direction from their larger customers who are subject to regulations and agreements. As a result, their cybersecurity practices are just enough to make their customers happy - which doesn't necessarily make the company secure. The risks that apply to the customer do not necessarily apply to the smaller company.

In addition to the lack of knowledge, many companies also have a lack of resources for cybersecurity. Large companies have teams who are responsible for cybersecurity, whereas a small company may have one person on the IT team that "sort of" knows security. Not only is there a lack of human resources, but there is also a lack of monetary resources. Larger companies have a budget for cybersecurity, and the human resources to implement a framework. Smaller companies may not have access to those resources. Unless there is an enforcement of some type - that affects the business, not just the IT team - the business will usually not spend money on cybersecurity. Fees, fines, lawsuits, and customers have so far been the business drivers of cybersecurity - not because companies are convinced that improved security increases value.

2.2 What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

There are many existing frameworks that can be useful. Trying to identify a single framework has issues as you move between sectors and countries. A company that is working internationally or in multiple sectors would welcome a single framework that would meet all of their customer's needs. This has not been the case for many organizations as each new customer has a different set of requirements - either from an existing standard or in-house developed criteria.

Threats and countermeasures lists also have problems - as the need to determine which items are relevant to an individual organization with all possibilities is overwhelming for an organization that is attempting to get started. People are unable to easily understand risk. Asking an organizational lead to determine the likelihood that an airliner will crash into their facility is unlikely to provide any valuable information. If instead guidance on expected possibilities was provided for each of the threats, an improved awareness of the threats could be realized. Creating a system that would allow ranges that could be updated based on changes in the world or current system attacks would provide the ability for companies to keep up with the ever-changing threat landscape.

Common problems with each of the frameworks are one or more of the following:

- Too difficult to start
- Gaps in the framework
- Frameworks that are too detailed
- Unknown level of effort (or known level of effort that is beyond resource levels)

With the unknown business information, supporters of risk management are unable to get the management buy-in that is required for a successful program. Providing guidance in a form that allows program support to get management buy-in and appropriate resources and budgets to protect the organization would help many organizations to get started on improving their security postures.

2.3 Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

No comment

2.4 Where do organizations locate their cybersecurity risk management program/office?

We've seen the cybersecurity risk management program located in multiple places within organizations. Most organizations we have evaluated locate their cybersecurity risk program under the IT group. Depending on the size of the company, it may be one "security" person on the IT team, or an entire group within the IT team. There may be some communication between the cybersecurity risk team and the business or enterprise risk management program, but we have not noticed this very often in the organizations we evaluate.

2.5 How do organizations define and assess risk generally and cybersecurity risk specifically?

The organizations that we have worked with that formally define and assess risk use a simple risk register and their imaginations (or the imaginations of their consultants). However; most of the organizations we have seen do not formally define risk, and rather assess their risk on an ad hoc basis, dealing with issues as they arise. Some work with their customers to define the "customer" risk and what risk level the customer is comfortable with in order to continue to do business with the company. In general, this is the limit of defining cybersecurity risk in smaller companies.

Those organizations that are subject to regulations that require a risk management program (such as HIPAA) are more likely to have one - at least documented if not implemented. Those that have customers that are subject to those regulations also tend to have a paper-based risk management process. However, we've noticed that this risk management process tends to be a one-time exercise, and not updated as threats evolve and change.

2.6 To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

To the extent that organizations have an enterprise risk management program, we see limited cybersecurity risk involved at the enterprise level. At the enterprise level, companies are focused on business risks - which may or may not involve cybersecurity. In some businesses, cybersecurity is a business risk that is considered as part of the entire enterprise risk management process. These businesses attract customers based on their perceived cybersecurity capabilities.

In most businesses, cybersecurity risk is limited to visibility within the IT department, and managed separately from the business risk.

2.7 What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

As most of our clients are in the healthcare industry, HIPAA and HITECH are two of the primary driving laws for practicing risk management. Some of the organizations we have evaluated follow ITIL, which includes minimal risk management, and others follow ISO 27001 - which also includes a risk management component. However, these standards are not applied equally. We tend to see ITIL in very large organizations with a completely separate or shared IT services group, and ISO 27001 in foreign companies, or companies that focus on non-US customers.

At the operational and technical levels, the cybersecurity risk is managed depending on the specific organization and the regulations and agreements they are subject to. Those that have agreed to PCI-DSS or SWIFT follow those guidelines and restrictions. Those with no regulation or agreement tend to follow vendor recommendations (i.e. Microsoft's hardening guides) or customer requirements.

2.8 What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

Regulatory and regulatory reporting requirements are highly dependent on the industry sector, and location of the company (or their customers). The primary regulations that we have seen deal with breach notification requirements - such as HIPAA and the Massachusetts Data Protection Law - and define who must be notified by when and if a breach does occur. While useful and necessary, breach notification regulations do nothing to proactively protect an organization's critical infrastructure.

HIPAA does require a minimal amount of cybersecurity through the Security Rule, but until recently, enforcement was limited to covered entities. It now applies to all business associates dealing with PHI, which has only slightly increased the scope, as covered entities were already required to meet Security Rule requirements through their business contracts.

2.9 What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

In general, we have found that the primary assets and services provided by the companies we have evaluated are primarily informational - involving both electronic information and human knowledge. Electronic information services cannot easily be provided without power, and only inconveniently without telecommunications.

Human knowledge is also important for most of the companies we have evaluated, and humans in general depend on critical infrastructure for basic needs. Most humans are not equipped to survive without power, clean water and money for extended periods of time. While states encourage citizens to be prepared for 3-4 days without in case of emergency, at that time, a citizen's focus becomes themselves and their families, not necessarily their employment. Without employees focusing on providing the human knowledge required for running their business, the business will not operate.

2.10 What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

What we have seen is that service level agreements (SLAs) do not necessarily take into account cybersecurity incidents. SLAs are generally agreed upon without input from the enterprise risk management team or the cybersecurity risk management team.

In most organizations, a disaster recovery scenario - in order to provide essential services - completely ignores cybersecurity. The goal is to get the systems or networks up and running at their minimal capabilities, and cybersecurity is not seen as a minimal capability, but rather as an "add on" that can be dealt with later.

2.11 If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

No comment

2.12 What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

We have seen that without enforcement or consequences, few companies are willing to spend the money, time, and effort,to reduce cybersecurity risk. At a minimum, there should be some enforcement activity that is supported by an international organization. Whether that is denial of membership, fines, or fees is better to left to behavioral economists to determine.

The international standards provide good guidance for federally regulated programs and can play a significant role in a risk management program for non-federally regulated entities. The standards could play a significantly more important role, if they were balanced with the legal expectations of organizations. Merely following the standard does not provide legal protection and in some cases may expose the organization to more risk than had the organization done nothing. This balancing of cybersecurity protections with legal defensibility would provide more incentive for organizations to use the developed standards.

The problem with this is that it is difficult to determine when a company has done “enough” to reduce cybersecurity risk. Some companies have limited funds to devote to cybersecurity, should that preclude them from competing with more well-funded companies?

Additionally, once there is a minimum standard or conformance requirement, many companies will do the minimum they are required to do to reduce liability, fees, fines and costs. Conformity assessments have a very large chance of becoming a “check the checkbox” task, without really considering or reducing risks.

3 Use of Frameworks, Standards, Guidelines and Best Practices

3.1 Standard Frameworks and Associated Problems

There are numerous citations that state that there are more than 800 different risk management frameworks with the three major approaches listed as ISO/IEC 27005, NIST SP 800-30, and OCTAVE. These three methodologies in particular rely on questionnaires, interviews, document reviews and/or workshops to work through the process.

Two of these frameworks have a set of suggested controls, ISO/IEC 27005 and NIST SP 800-30. Instead of evaluating risk this has instead lead to organizations attempting to meet all of the controls. Many of the controls may be irrelevant for a particular organization and/or system, but due to the unknown abilities of the future ISSO or assessor, the risk management process decides that there is less risk of not passing the audit if all of the controls are implemented.

The process of implementing all controls goes against the concept of risk management and moves instead to a process of risk avoidance as the only strategy. This uses an organization's limited resources in an inappropriate manner. This process comes out of fear and misunderstandings of how to implement cybersecurity.

The European Network and Information Security Agency (ENISA) provides a comparison of some of the available Risk Management Methods and Risk Management Tools. NIST and other country-specific methodologies appear to be missing or excluded from the list of available Methods and Tools. A shortcoming is that the comparison does not provide a means to filter the methods based on any criteria and instead requires the reader to sift through the results to determine appropriateness.

ISO 27005 describes a management-based approach to risk, hinged on the identification of risks and estimation of their impact.

Because of the broad nature of the standard, ISO 27005 can be used by many companies in almost any sector. The standard document itself is brief, defining the iterative approach to risk identification and estimation, leaving the implementation largely up to the organization. In some ways, this makes the standard more accessible to organizations of different sizes and capabilities.

However, this broad nature can also be seen as vague, which limits the impact of claiming ISO 27005 compliance. Because there are no strict requirements in ISO 27005, simply being ISO 27005 compliant means little to an outsider without a more in depth knowledge of the specific risk management strategies being used.

As with all other ISO standards, ISO 27005 suffers further from being a closed standard. With access to the definition of the standard restricted only to paying customers, fewer business partners or other outside entities can fully understand what compliance entails.

ISO 27001 and 27002 are ISO/IEC standards that detail the requirements for establishing and operating an Information Security Management System. ISO 27001 details the overall requirements for the ISMS, and ISO 27002 explains the code of practice for operating the ISMS. Because the ISO 27002 standard only describes how to run the system, as opposed to ISO 27001, which describes the ISMS itself, an organization cannot be certified against ISO 27002; certification is only available for ISO 27001.

These standards offer a rigorous set of precise controls that a company can address in order to be compliant. Unlike ISO 27005, the requirements of ISO 27001 combined with the code of practice guidance in 27002 provide both specificity and flexibility in selecting an implementation strategy commensurate with the level of acceptable risk. For example, for a given requirement of ISO 27001, ISO 27002 provides a list of possible controls that can be implemented. An organization can decide which of these controls to implement, or even none of them, as applicable to their needs.

However, the list of requirements and controls is rather long, and is a cumbersome undertaking for a smaller organization. While it is possible to achieve certified compliance with ISO 27001, smaller organizations may find the documentation and organizational efforts too involved for their needs, as well as finding the certification process too complicated and expensive.

Similar to ISO 27005, these standards also suffer from being closed. The value of the standard is diminished somewhat, as the number of outside entities, including business partners and customers, can understand what ISO 27001 certification means without access to the requirements of the standards.

Some software vendors publish security guides that offer advice and best practices for securing their products. Many organizations at least glance at these guidelines when installing these products. In some cases, adherence to the vendor guidelines is required for vendor support, which incentivizes companies to follow them.

3.2 Checkboxes Aren't the Answer

In our organization, we believe that checkboxes are not the answer to better security. Whether your checkboxes are the ISO 2700x, NIST 800-30, PCI DSS, or HIPAA security controls, doing risk management by making sure all the boxes are checked is counter-productive because they are incomplete, insufficient, and dangerous.

Incomplete: Doing risk management by ensuring all the boxes are checked removes a lot of the value of the process because it assumes a "one size fits all" set of checkboxes. It is unrealistic to think that the information security needs and practices of every organization necessarily need to be the same. It also cannot take risk tolerance into account. In some cases a risk management process makes a decision that might save a few dollars, and in other cases risk management processes make decisions that might save lives. Checklists cannot capture a narrative as to what is and is not being performed, nor can they easily capture compensating or mitigating controls that might be in place.

Insufficient: Limiting a risk management process to checkboxes eliminates the ability to capture other valuable information, including things like reports, network diagrams,

presentations, and educational or awareness materials. Checkboxes remove the art and subtlety of risk management that allows those with more experience to understand and influence a risk management decision. And since checkbox-based risk management is insufficient, it results in many different sets of checkboxes. It is this very fact that seems to have caused this RFI to be created, in order to find the "best" set of risk management methodologies, aka checkboxes.

Dangerous: The most concerning problem with focusing risk management on checkboxes is the fact that important information can be concealed through its absence in the list. While performing a physical security assessment in the pharmaceutical industry, a colleague was presented with a problem. The building met all the requirements of the checkboxes that were his goal for the assessment; however, he could not consider the building to be physically secure. The reason was that there was a hole in the side of the building from a crane accident earlier in the week. There was no checkbox with a question that would reveal a hole in the side of the building. According to the checkboxes, the building was secure, but any person could see why it was not. In addition to not being able to illuminate any problem that is not directly addressed by a checkbox, there is no ability to prioritize between the value of different questions and answers. If a risk management methodology consists of 300 questions, and the ability to secure information is judged by how many of those answers are "right", it can create a tremendous flaw. It is possible that the organization that has 299/300 correct presents a higher risk than the organization that has 250/300 correct, because the one question missed by the first organization could cause the complete bypass of all the organization's other controls.

It is therefore our recommendation to NIST that the result of this RFI exercise is **not** a new, more comprehensive set of checkboxes. Instead, the focus should be placed on how to consistently capture the information that *cannot* currently be captured by checkboxes, and how the value of that information could be shared to improve cybersecurity within critical infrastructure and throughout public and private sector organizations across the nation.

4 Specific Industry Practices

4.1 Are these practices widely used throughout critical infrastructure and industry?

Most of the practices listed above are not widely used throughout the companies and industries we have evaluated. For example, mission/system resiliency practices are only common in large data centers and large companies where it is generally limited to high availability. In general, we have found that small companies do not have the monetary resources to pay for the high availability offered by their hosting companies, so they choose to not pay for those services.

Encryption and key management is only used within organizations that have a regulatory requirement to use encryption. Some smaller companies have chosen to use Windows Bitlocker/EFS or Apple's FileVault as part of their normal practices, just because they are offered. However, these technologies are used without fully understanding the implications; for example, there is generally no way for the IT team to decrypt the drive if necessary.

Most organizations have a minimal monitoring and incident detection capability. We see that most organizations have logging enabled on their systems (generally because it is the default), but only look at those logs when trouble arises. Almost universally, logs are not reviewed on a regular basis, unless there is an entire team dedicated to security operations (such as at a data center). We are starting to see this change with more Security Event Information Management (SEIM) and Security Event Log Monitoring (SELM) tools becoming available and widely deployed. The larger organizations we have evaluated have begun this process, and the requirements are slowly making their way down to the smaller business partners.

We have found that many organizations do not have formally defined incident handling policies and procedures; they would "wing it" if necessary. Some organizations have an extensive system in place due to regulations (HIPAA's breach notification rule being a common requirement), and may have had to use it. Most organizations we have evaluated have to think about what they might do in case of an incident. We recommend that at least a minimal plan be available so that decisions are not rushed in hectic response.

Security engineering practices are almost unheard of in most of the organizations we have evaluated, with those that do have a security engineering practice being development companies. A formal user and requirements testing process is almost universal, but rarely is cybersecurity considered in the requirements. Some larger organizations that manage multiple products have instituted a formalized software/system development lifecycle which includes testing a set list of security requirements.

Most organizations (depending on the service they are providing customers) do separate their business systems from operational systems. It has long been a best practice from research and development (R&D) days not to touch anything that's working, so operations were not touched unless absolutely necessary. The thinking on this has not changed much. There is still very much a "don't touch what's working" mindset, but the separation of business and operations systems allows the R&D teams to play around with what they need, while leaving what's working alone.

Two of the practices that we see almost universally are identification and authorization of users and asset identification and management. At the minimum, every user has a login credential (generally tied to an Active Directory) and logs in with those credentials for identification and authorization. This is generally the extent of what we see, though.

Authorization is a little less defined in these organizations. For the most part, if you are a domain member, you have permissions to access most information assets and services. There may be a special user group carved out for the HR team - so that only the HR folks can access those assets and services - but that is usually the limit of access control.

Physical asset identification and management is driven less by cybersecurity needs and more by financial needs and the ability to depreciate the physical assets. Virtual assets are less well-managed. The software that has been paid for is managed, but specific information, documents or services may not be identified or managed. In some organizations where the IT team and the finance teams do not communicate well, the IT team has access to a list of computers based on their domain membership in Active Directory; that's their asset list.

Finally, we see a wide variation in privacy practices (we haven't evaluated any companies where civil liberties would be affected). A majority of the companies we have evaluated are related to the healthcare industry and are very familiar with HIPAA and other medical privacy regulations. The companies that deal with PHI are cognizant of their duty to protect individual data. Those that are working on the periphery and not directly dealing with PHI are less likely to be aware of the value of the data they are handling.

4.2 How do these practices relate to existing international standards and practices?

No comment.

4.3 Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

We believe that security engineering, system resiliency, and monitoring are the three most critical practices for the secure operation of critical infrastructure in any sector.

Security engineering can be used to prevent against many known attacks and vulnerabilities just by designing security into the system. Starting with a defense-in-depth mentality is a lot easier than adding one after the fact. That leaves less security "bolted on" after the fact, which is less effective and more expensive. Given the fundamental definition of critical infrastructure, it is important that those services continue to be provided during emergencies and cyber-attacks.

System resiliency allows organizations to continue providing those services when needed. However, defining a good cost-benefit ratio for resiliency will be a difficult problem to resolve.

Finally, monitoring for incidents is extremely important and often overlooked. General logging is enabled on systems, but organizations often do not have the resources - or the resources do not have the necessary skills - to review those logs regularly. Monitoring for an incident does not prevent an attack, but it can help mitigate the effects of the incident by allowing other processes to protect the asset or the remaining assets.

4.4 Are some of these practices not applicable for business or mission needs within particular sectors?

While all of the organizations we have evaluated have considered their business/data availability, many decide that their data and the services they provide are not critical, and can withstand a lengthy outage. We see that mission/system resiliency is not commonly adopted among the companies we have evaluated. This is not sector specific, but more of a financial resource constraint.

We believe that in the general case, these practices are applicable to all sectors, but not necessarily to all businesses within those sectors. We believe that these practices should be considered as part of a holistic information security management program, but the specific controls implementation and decisions should be based on the risks each protects against.

4.5 Which of these practices pose the most significant implementation challenge?

Which practice poses the most significant implementation challenge seems to depend on the organization. In general, we see issues with encryption and key management across sectors and companies. There are so many ways to implement key management and so many vendors offering products that the hurdle is often deciding how to do it. Once the encryption and key management has been operationalized, we generally do not see issues with it.

The practice that we see with the most operational implementation challenges is monitoring for incidents. This is a primarily operational task that requires human resources to review logs and alerts, or financial resources to outsource the task to software or another company. The lack of resources is the biggest challenge to implementing monitoring. Monitoring is not generally seen as a core business function, and so it tends to be lower on the list of operations to get funding. Many companies outsource this task as part of a managed services agreement for various hardware or devices (usually the firewall or intrusion detection system).

4.6 How are standards or guidelines utilized by organizations in the implementation of these practices?

Vendor guidelines are very commonly used for implementing these practices, but that requires a company to have previously made the decision to implement that practice and purchase a product that helps them do that. In some sectors - specifically federal - the NIST standards are followed and sometimes required by customers. In healthcare, we see the HIPAA security rule being followed, and in most financial companies, PCI is being used.

However, all of these examples have something in common: these companies are required by law, by association, or by their customers to follow these standards and guidelines. This underscores the importance of an effective enforcement, even if it is informal between businesses and their customers.

4.7 Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Only the very large organizations we have evaluated have such a methodology. Most that we have seen follow ITIL as an international standard.

Some of the smaller European and Asian based companies we have evaluated have spent the time and effort to become ISO 27005 certified, but we very rarely see this within the United States, even with larger organizations.

4.8 Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Most of the smaller organizations we have seen do not have an escalation process. Even where the smaller company does have some sort of incident response process, it generally does not include an escalation process. The larger organizations with a formalized incident response system generally do have such a process.

4.9 What risks to privacy and civil liberties do commenters perceive in the application of these practices?

No comment.

4.10 What are the international implications of this Framework on your global business or in policymaking in other countries?

Having a global framework would be useful for many businesses that operate globally or with international partners. This would eliminate the need to map different frameworks to each other and may eliminate the need for multiple audits. However, without a broad adoption, there will still be many of the same issues we see today.

4.11 How should any risks to privacy and civil liberties be managed?

No comment.

4.12 In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Related to security engineering, a defense-in-depth approach should be considered. While security engineering should include or imply defense-in-depth, it generally does not. Many organizations have a solid perimeter, but a soft squishy center. Once an attacker breaches the perimeter firewall, they can gain access to almost anything. The defense-in-depth approach also allows for more resilience; it takes more than one attack to deny access to a particular service.

We also believe that vendor management must be a security practice considered within the framework. It is rare that a business does everything “in-house”. Many business functions are outsourced to other companies; payroll, customer support, marketing, and IT are areas we see commonly outsourced. Each company must evaluate their risk and the risk of allowing another company access to their sensitive information, and work with the outsourcer to resolve or mitigate that risk. As with risk in general, the solution will change from sector to sector and company to company, but the potential for risk must be considered. Depending on the company that is using business services, the folks responsible for cybersecurity may not be involved in the vendor selection process to determine the risk and appropriate controls for that risk.