Deloitte.

Changing the game on cyber risk

The path to becoming a more secure, vigilant, and resilient agency

Contents

Introduction	1
Becoming secure: Fortify the agency	2
Remaining vigilant: Manage the inevitable	3
Being resilient: Prepare for the unpreventable	4
Getting governance right	5
Where to start	6

Introduction

The cyberthreat landscape continues to evolve, with increasingly determined and sophisticated attackers. At the same time, agencies are spending more money and paying more attention to cyber than ever before.

Yet the problem of cyberattacks persist, amid an increasingly complex cyberthreat landscape where agencies continue to trek deeper into the digital realm—adding new layers of connectivity and interaction between themselves and their constituents.

Both the economy and our society-at-large have become connected using platforms designed for *sharing* information, not *protecting* it – presenting new opportunities every day for would-be attackers. And the very things organizations do to innovate and grow will actually create or magnify cyber risk.

Risks today extend far beyond theft and fraud to include loss of competitive advantage due to stolen intellectual property, loss of citizen or constituent trust, and overall damage to an agency's reputation and brand. Managing cyber risk has become a strategic imperative that has profound implications for the overall performance of the enterprise. And the complexity of the risk will only grow as the vision of the Internet of Things continues to take shape. More connected devices, more sources of data, more process automation, and more third-party relationships will help create new layers of opportunities for cyberattackers.

Organizations will have to move far beyond a "secure the perimeter" mentality and begin incorporating cyber risk thinking into their product design and engineering processes—taking a long-term view of what it means to be secure.

As cyber incidents and their associated costs continue to rise, there's a growing realization that becoming impenetrably secure is impossible in today's environment. It is almost inevitable that safeguards will sometimes fail. Managing cyber risk is not a one-time solution. It is an ongoing journey—for information technology (IT) leaders and decision-makers alike—to take meaningful steps to change the game on cyber risk.

Cyber risk management is an enterprise-wide concept that encompasses the IT-centric discipline of cybersecurity as well as a broad set of risks that have strategic, operational, and regulatory implications. Effective cyber risk management focuses on assessing threats, vulnerabilities, and their potential impact on the broader agency. Ultimately, cyber risk management is inextricably linked to an agency's ability to effectively deliver its mission.

Moving toward a more secure, vigilant, and resilient agency

Because you can't prevent all cyber incidents, agencies need to be secure, vigilant, and resilient. With many organizations today already breached by cyberattackers—and with many unaware of the breaches—realistically assessing your agency's changing risk pro ile becomes critical, to help determine what levels and types of cyber risk are acceptable. Through the lens of what's most important to your organization, agencies today should invest in cost-justified security controls to protect their most important assets, while also gaining more insight into threats and responding more effectively to reduce their impact.

At a glance: What does it means to be secure, vigilant, and resilient?

Secure

Establish and continually maintain foundational security capabilities —by enhancing risk-prioritized controls to protect against known and emerging threats, while also complying with industry cyber standards and regulations.

Vigilant

Detect violations and anomalies through better situational awareness both externally and across your environment —spanning all areas of your ecosystem.

Resilient

Establish and exercise the ability to quickly return to normal operations and repair damage to the agency following the inevitable cyberattack.

Becoming secure: Fortify the agency

Being secure means focusing protection around the risk-sensitive assets at the heart of your agency's mission. Traditional security controls, preventive measures, and compliance initiatives probably have consumed the greatest part of your investment in cyber risk management, and you will most likely need to continue—or increase—your investment levels.

But as you engage in these core cyber "hygiene" activities, you might need to rethink your decision criteria. Malicious actors, especially those motivated by financial gain, tend to operate on a cost/reward basis. If your defenses are strong enough to raise their risks (and level of effort relative to the value of what they can gain), they are more likely to turn their attention elsewhere.

"Value" is a pivotal qualifier

Given the reach and complexity of your digital ecosystem, you can't secure everything equally so focus protection around the risk-sensitive assets at the heart of your agency's mission—the ones that both you *and* your adversaries view as highest value. Among the most important elements are critical infrastructure, applications, and data, as well as specialized control systems. Also remember that these elements are part of larger services and transaction chains, and addressing weak points along the end-to-end business process is essential.

Don't allow gaps to leave you exposed

Many agencies can significantly improve cyber risk management by instilling fresh discipline in some basic areas, such as data tracking and classification. Another common and closely related area of weakness is asset management. Large agencies generate enormous change on a daily basis—new users, new devices, new applications, and supporting changes to the underlying infrastructure. If security controls are not adjusted to keep pace, you're likely to create gaping holes that can leave your agency exposed for days, months, or even years.

Non-negotiable areas to fortify

Most cyberattacks exploit *well-known* system weaknesses—known to hackers and known to the organizations they target. You can address such weaknesses by administering a comprehensive patch-management program that focuses on critical data assets using a risk-based approach, rather than an ad hoc or compliance-based approach. Some other areas to fortify: software development, IT asset management, and physical security. Agencies should add protocols and a security mindset to the development and asset management processes. They also should work to spot physical security holes and weaknesses that could allow an unauthorized individual, a disgruntled worker, or an unwitting employee to leak or steal critical information.

Security starts at the top: Put a senior leader at the helm

Above all, fortifying your agency will require a strong leader to drive cohesive, decisive action. Establishing a solid cyber foundation requires someone with broad influence who can generate collaborative engagement among the diverse range of players essential to the success of the program—many of whom might be unaccustomed to thinking about cyber risk. Who should take the lead? You want someone who not only understands the mission, but who can also manage risks and authoritatively drive a transformation agenda. Someone who can enable innovation, eliminate obstacles, and support growth—all the while taking the necessary steps to prepare for the possible outcomes.

Remaining vigilant: Manage the inevitable

Cyber hackers continue to show an abundance of motivation. They need to be successful only once to see a payoff for their efforts. But your agency must be successful in managing the inevitable attacks every time—with an emphasis on slowing or minimizing the impact of an attack so your agency can respond and recover more effectively. Today's costliest attacks tend to be the ones that are highly targeted, for specific reasons.

The need for context

As security operations centers collect terabytes of data and generate tens of thousands of daily alerts, analysts can become overloaded. Details might be important, but without context, it is impossible to know if you're seeing what really matters. Moreover, you might be spending time assessing data and alerts that do not matter—that are irrelevant to your agency. For example, if certain threats apply only to software that your organization is *not* using, you can eliminate a cycle of "noise" about those threats and instead focus resources on more pressing needs. Examining pertinent use cases or indicators and then correlating them with the realities of your operations can help bring more relevance to your efforts.

Detect, plot, and translate the cyberthreat landscape

Develop a solid picture of what you need to defend against. Understanding the unique government landscape is an important starting point that needs to be supplemented by an understanding of your agency's specific risks. It's a broad exercise to examine who could harm you, what motivates them, and how they're likely to operate. By carefully plotting the motives and psychology of adversaries, and considering the potential for accidental damage by well-intentioned constituents, partners or employees, cyber risk strategists anticipate what might occur and design detection systems accordingly.

This is not just a technical challenge. Department and agency leaders need enough understanding of the cyberthreat landscape to provide cyber risk guidance. It is then the job of technical teams to translate this into effective operational capabilities. As you develop vigilance and related cyberthreat intelligence (CTI) capabilities, work to ensure that you are constantly evolving those capabilities to adapt to the evolving threats.

Know what you're protecting

Fending off an attack begins with knowing what you *need* to protect, not just what you *want* to protect. As you seek to identify your critical assets and become more vigilant about protecting them, think outside the walls of your organization—to include contractors, vendors, and suppliers. Don't rely too heavily on a vendor questionnaire. Ask your partners and potential partners for security audit reports—and consider conducting regular site visits, based on criticality of assets they access or host. It's up to your agency to assess what the loss of data will mean. You'll also need to develop layers of awareness within your organization to ensure that employees are aware of the threats, the risks, and their roles in managing them.

Vigilance depends on insights: Develop cyberthreat intelligence

To address cyberthreats effectively, agencies should have a cyberthreat intelligence (CTI) capability that will help them rapidly identify, detect, and respond to threats. CTI involves proactively acquiring, analyzing, and disseminating intelligence as a way to minimize risk. The amount of intelligence can be overwhelming, so organizations should focus on what matters most to them—intelligence with relevant value. The most effective CTI programs tend to be those that apply clear mission context to the data they collect and then develop insights that are actionable.

Being resilient: Prepare for the unpreventable

Being resilient means having the capacity to rapidly contain damage—to slow down the unpreventable attack while mobilizing the diverse resources needed to minimize mission impact, including direct costs and service disruption, as well as reputation and brand damage. Your efforts should be thorough and agency-wide.

Thinking ahead

Get started by asking forward-looking questions. You might have a security-incident-management process in place, but have you tested it? When (not *if*) your agency is attacked, how will you respond? How will the IT department react? How will the operational side of your organization—and the communication arm of your organization—react? How will they work together to understand the problem, remediate the problem, and let partners and constituents know what's going on?

Communication and planning

While resilience requires investment in traditional technology-based redundancy and disaster recovery capabilities, the bigger picture includes a complete set of crisis management capabilities. It involves IT, of course, but also various agency and department leaders, as well as decision-makers from legal, risk, human relations, and communications functions. It requires a playbook across all these entities, designed in advance by considering how threat scenarios affecting critical assets and processes could play out.

Make practice a priority

Rehearse playbook tactics and policies through cyber wargaming and simulations that bring together technology teams and other key agency stakeholders. Staging simulations creates better organizational awareness and understanding of threats, improves cyber judgment, and develops "muscle memory" that helps teams respond flexibly and instinctively to both the scenarios you envisioned, and the situations that couldn't be foreseen.

Such simulations involve not only technology, but also the people involved in responding to incidents. Agencies should include their operational staff and upper-level leadership in simulations. Simulations could also involve independent "red teams" that are highly informed on current threats and that can engage in relevant and realistic exercises designed to help assess your vigilance and response capabilities.

Ultimately, resilient agencies take the time to absorb important lessons, and modify the secure and vigilant aspects of the program for continuous improvement.

Resilience requires constant improvement: Generate some momentum with early 'wins'

One smart strategy for jump-starting a "constant improvement" capability: launch priority projects that can deliver early "wins" for your cyber risk program. Doing so can help you establish momentum by focusing on several areas or pilot initiatives that directly influence success or mission achievement, with objectives that can be measured, and with built-in continuous improvement processes.

Getting governance right

Becoming a more secure, vigilant, and resilient agency requires effective governance through a program tailored to your agency, with several core common characteristics:

They are executive-led

Agency and department leaders should set the stage by defining cyber risk management priorities, risk appetite, and mechanisms of accountability. Sponsorship at the top is essential in rallying diverse groups and departments to collaborate in new ways.

They involve everyone

Although specific roles should be well-defined, the program is not the sole responsibility of a single part of the agency. It requires broad horizontal and vertical participation, and behavioral change throughout the agency.

They're programs, not projects

Although it usually requires a series of projects to get off the ground, the secure, vigilant, and resilient approach is an agile and adaptive program requiring continuous review and improvement cycles to adapt to changes in the risk and cyberthreat landscapes.

They are comprehensive and integrated

The secure, vigilant, and resilient elements are not distinct silos of activity. They're a set of lenses through which every essential agency process and growth initiative should be evaluated or planned. Each involves people, process, and technology components. Executed well, each will improve the others.

They reach beyond your walls

Your ecosystem includes various partners, suppliers, and vendors. Significant cyber incidents directly affecting them might also substantially affect you. These transformations can't take place without strong governance. Instituting a secure, vigilant, and resilient program requires a carefully guided evolution—changes in roles, processes, accountability measures, well-articulated performance metrics, and, most of all, an agency-wide shift in mindset.

Where to start

Where to begin with improving your cyber risk profile will depend on where you are today. If you're in the early stages of a transformation process, the following additional steps can help you move in the right direction:

Map threats to the agency assets that matter

Create a high-level cyber risk guidance matrix by gathering top agency leaders and threat intelligence specialists. Together preemptively discuss the potential threat actors and trusted insiders who could cause harm, the damage they could impose, and how they might do it. Then identify significant areas of unaddressed cyber risks, set your risk appetite, and prioritize program areas.

Accelerate behavioral change through incentives and experience-based awareness

Traditional security training is an important program component, but on its own is not enough. A policy manual alone will not prepare people to take the right action, so create active learning scenarios that deepen understanding of the impact of day-to-day activities on the agency's cyber risk posture, and identify visible opportunities to reinforce the right behavior through programs that reward speaking up, raising questions, and achieving program objectives.

Agencies cannot afford to slow innovation simply because they cannot be perfectly secured. But neither can they innovate without appropriate regard for the inherent risks being generated. Cyber risk and innovation are inextricably linked; rather than subordinating one to the other, senior leaders must harmonize these important elements of agency performance through a program to become secure, vigilant, and resilient.

For more information, please contact:

Deborah Golden
Principal
Federal Cyber Risk Services Leader
Deloitte & Touche LLP
debgolden@deloitte.com

Deloitte has been widely recognized as a market leader, including these recent independent analyst reports:

- **Deloitte named a global leader in Security Operations Consulting by ALM Intelligence**
  Source: ALM Intelligence; Security Operations Center Consulting 2015; Kennedy Consulting Research & Advisory estimates

- **Deloitte ranked #1 globally in Security Consulting, based on revenue by Gartner**
  Source: Gartner, Market Share Analysis: Security Consulting, Worldwide, 2015, Jacqueline Heng, Elizabeth Kim, April 2016.

Deloitte.