Deloitte.

Changing the game on cyber risk
The imperative to be secure, vigilant, and resilient

Contents

Introduction

The strategic things you do to achieve your mission are at the heart of the cyber risks your federal agency faces.

Most reports on cyber security revolve around a common theme: despite heightened attention and unprecedented levels of security investment, the number of cyber incidents — and their associated costs — continues to rise. They typically point to the growing sophistication of hackers and other adversaries as a particularly intractable problem, and some deliberate over whether being secure is even possible in today's rapidly evolving landscape of cyber attacks.

Important questions, though, remain unaddressed. In particular: what are the underlying reasons for this trend and how can federal agencies actually reverse it to start winning the cyber risk battle?

The first question has a lot to do with your agency itself, and is not just about the sophistication of external actors. Over the past two decades, we have woven a fabric of connectivity in our economy and society via the Internet — a platform that was designed primarily for sharing information, not protecting it.

Your agency has doubtless benefitted from this connectivity — driving innovation, efficiency, and performance that were unthinkable a generation ago. You've likely used it to transform relationships with constituents or overcome geographic constraints. Or perhaps it's enabled you to gather data that shape your strategy, automate diverse operational systems, or launch new services.

This increasing digital reach adds layers of complexity, volatility, and dependence on infrastructure not fully within your control. Your efforts to grow, serve, and streamline introduce new gaps and opportunities that attackers will try to exploit — because your adversaries, too, leverage the Internet to accomplish much more, much faster, and from anywhere. For every step you take, they will be close behind. In short, the strategic things you do to achieve your mission are at the heart of the cyber risks your agency faces.

When we consider this inherent link between agency performance, innovation and cyber risk, it becomes clear that protecting everything — while perhaps not impossible — would be economically impractical and would likely impede some of your most important strategic initiatives. Some cyber incidents will occur. Every agency must realistically assess its changing risk profile and determine what levels and types of cyber risk are acceptable. Managing your cyber risk is not a necessary evil, but an essential aspect of enabling optimal performance.

This brings us to the second question and the central theme of this paper. Namely, how can federal agencies reverse the growing gap between security investment and effectiveness in a world where it is not feasible to be 100 percent secure?

Given that you cannot prevent *all* cyber incidents, the traditional discipline of security, isolated from a more comprehensive risk-based approach, is not enough to protect you. Through the lens of what's most important to your agency, you must invest in cost-justified security controls to protect your most important assets, but you must focus equal — in some cases greater — effort on gaining more insight into threats, and responding more effectively to reduce their impact. Through an ongoing program to become *secure, vigilant, and resilient*, you can be more confident in your ability to reap the value of your strategic investments.

Being secure

You can't secure everything equally. Being secure means focusing protection around the risk-sensitive assets at the heart of your federal agency's mission.

Traditional security controls, preventive measures, and compliance initiatives have probably consumed the lion's share of your investment in cyber risk management, and you will most likely need to continue — or increase — your investment levels, because the stakes have never been higher.

But you may 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. Being secure means focusing protection around the risk-sensitive assets at the heart of your agency's mission — the ones that both you and your adversaries are likely to agree are the most valuable.

Among the most important elements are critical infrastructure, applications, and data, as well as specialized control systems — but they're not isolated components. They're part of larger services and transaction chains, so it's essential to address weak points along the end-to-end process, with the awareness that insiders, vendors and trusted partners at any point can be the source of errors or intentional actions that open the door to incidents.

If you've historically underinvested in security, this should be remedied, but improving security is not always about spending more money — and it's also not just about buying the latest security tools. Many agencies can do significantly better by instilling better discipline in some basic areas.

One is data tracking and classification. Many agencies don't know where their sensitive data actually resides. It's probably sitting in more places than you think — both inside and outside your agency — being viewed and shared by more people than necessary. Effort should be taken to streamline and control access wherever possible.

Another common and closely related area of weakness is asset management. Many 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.

A closer look

Strong asset management is a significant enabler of *secure, vigilant, and resilient* practices.

For example, proper reconfiguration and decommissioning of laptops and servers is critical in preventing data leakage. Mature processes maintain up-to-date tagging of critical assets that support high-risk areas.

This intelligence can be used in conjunction with monitoring technologies to prioritize attention to security alerts — helping analysts discern the difference between a minor event and one that could potentially escalate into a crisis.

Being vigilant

By carefully plotting the motives and psychology of adversaries, and considering the potential for accidental damage, cyber risk strategists anticipate what might occur and design detection systems accordingly.

Today's costliest attacks tend to be the ones that are highly targeted — at you, for specific reasons. Being vigilant means establishing threat awareness throughout the agency, and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets.

Collecting terabytes of data, security operations centers can generate tens of thousands — sometimes literally millions — of alerts daily. Analysts are overloaded partly because detection is focused on infected machines, malicious IP addresses, or failed login attempts. Those details may be important, but without context, it is impossible to know if you're seeing what really matters.

Yesterday's relatively isolated malicious activity has given way to well-organized cyber crime enterprises and networks of politically motivated, and sometimes state-sponsored, attackers. They might steal data for financial gain or disrupt critical infrastructure to cause chaos or inflict economic damage. Relentless, sophisticated and patient, they stage attacks over time until they get what they're after. Sometimes your employees or partners — wittingly or inadvertently — are accomplices.

Your efforts to be vigilant starts with 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 threat landscape to provide cyber risk guidance. It is then the job of your technical teams to translate this into effective operational capabilities. And these capabilities must be continually adapted. Every innovation creates new possibilities that misuse or abuse will occur. And for every innovation, and every new control put in place, malicious actors will try to find the cracks and seep through them; you must adjust and preempt them.

A closer look

Detecting persistent and targeted threats requires broad agency-wide collaboration, and therefore strong governance.

First, because they require ongoing access to a very broad range of data — not just from IT devices and systems, but also information as diverse as employee rosters, constituent usage patterns, inventory records, financial records, and potentially data from non-traditional digital sources such as facial recognition systems, facilities access records, telephony records, industrial control systems and the list goes on.

Second, the designers of these capabilities require deep engagement with department and agency leaders to understand what "normal" activity and indicators of risk look like.

A closer look

Malicious insider attacks are not impulsive. Rather individuals move on a continuum from ideation to action, exhibiting certain behavioral indicators along the way. Insider acts often trigger potential risk indicators in three categories:

- Virtual actions, such as emails sent and databases accessed;
- Non-virtual actions, perhaps unexplained absences; and
- Contextual descriptors, such as user access and privileged rights.

Revealing at-risk employees requires correlation of data across these categories to connect the dots to discover relevant patterns over time.

Being resilient

If response to cyber incidents is viewed as primarily a technical function, you will likely not be equipped for decisive action.

Your technical teams handle many day-to-day, fairly routine security events. But some incidents may become serious crises, which can affect your agency's broader mission. Being resilient means having the capacity to rapidly contain the damage, and mobilize the diverse resources needed to minimize impact — including direct costs and service disruption, as well as reputation and brand damage.

If response to cyber incidents is viewed as primarily a technical function, you will likely not be equipped for decisive action on whether or not components of your operations should be taken off line, what to report to authorities, and how to collaborate with law enforcement. You may also be less nimble in resuming normal operations and less able to manage the perception of the public and other stakeholders.

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, and 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 impacting critical assets and processes could play out.

Playbooks and policies must be written, but it's equally important to rehearse them through cyber war-gaming 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 plants the seeds of "muscle memory" that helps teams respond flexibly and instinctively to both the scenarios you envisioned, and the situations that couldn't be foreseen.

Finally, incident response and crisis management must feed continuous improvement processes. Resilient agencies take the time to absorb important lessons, and modify the secure and vigilant aspects of the program to emerge stronger than before.

A closer look

Cyber war-gaming exercises reveal common issues that cause delays in responding as rapidly and effectively as a real crisis situation would warrant:

- Groups accustomed to operating in silos face challenges in coming to agreement on the relative severity of an incident, and therefore of the key actions needed.
- Roles and responsibilities, though they may be outlined in a process manual, are not well understood.
- Lack of awareness of law enforcement structures and legal process causes failure to capture valuable forensic evidence.

It won't work without governance

A *Secure.Vigilant.Resilient.*™ cyber risk program is not just about spending money differently – it's a fundamentally different approach.

Transforming from a traditional, standards-driven IT security program to a *Secure.Vigilant.Resilient.*™ cyber risk program is not just about spending money differently—it's a fundamentally different approach — and your program will be unique to you. The balance of investment in *secure, vigilant, and resilient* capabilities will vary between agencies, and will even be applied differently to the various areas within your agency.

That said, *Secure.Vigilant.Resilient.* programs have some common characteristics:

- **They are executive-led.** Department and agency leaders must 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 need to 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, *Secure.Vigilant.Resilient.* is an agile and adaptive program requiring continuous review and improvement cycles to adapt to changes in the risk and threat 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. And done well, each will improve the others.
- **They reach beyond your walls.** Your ecosystem includes various partners, suppliers, and vendors; significant cyber incidents directly impacting them may also substantially affect you.

These transformations can't take place without strong governance. Instituting a *Secure.Vigilant.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.

A closer look

It's a living thing. Any initiative where risk-sensitive areas of the agency are enabled by digital assets should be considered through a *secure, vigilant, resilient* lens. Examples might include:

- A Chief Medical Director decides to empower the medical workforce and local affiliates with mobile medical devices;
- A project team is charged with consolidating equipment and revising agency network access for employees and contractors as part of a significant organizational realignment effort;
- A Chief Information Security Officer enables the employee and contractor workforce with a bring-your-own-device (BYOD) mobile device approach to individuals accessing agency workspace(s).

Walking the talk

In the pace of today's climate, federal agencies cannot afford to slow innovation simply because it cannot be perfectly secured. But neither can they innovate without appropriate regard for the inherent risks being generated.

Where to begin will depend on where you are today, but if you determine that you're early in a transformation process, the following steps can help you move in the right direction:

1. **Put a senior leader at the helm.** A cyber crisis situation requires a strong leader to drive cohesive, decisive action. But establishing the foundation requires someone with broad influence who can generate collaborative engagement among the diverse range of players essential to the success of the program — most of whom may be unaccustomed to thinking about cyber risk. The person in charge of the *Secure. Vigilant.Resilient.* program must be able to lead in both capacities, and be respected among a wide range of leaders, and at the board level.

2. **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 to preemptively discuss the potential threat actors and trusted insiders who could cause harm, the damage they could impose, and how they might do it. Through this threat-centric lens, identify significant areas of unaddressed cyber risks. Set your risk appetite and prioritize program areas that embody your strategy for becoming *secure, vigilant, and resilient*.

3. **Launch priority projects for early "wins."** Establish momentum by focusing on several areas or pilot initiatives that directly impact agency success or mission achievement, with objectives that can be measured and enabled through continuous improvement processes. By maintaining focus and demonstrating results, you can plant the seeds of a *Secure.Vigilant.Resilient.* culture that has a long-term, sustainable impact.

4. **Accelerate behavioral change through incentives and experience-based awareness.** Traditional security training is an important program component, but on its own is not enough, as evidenced by the number of breaches that can be traced back to stolen laptops, weak passwords, or failure to follow secure application development protocols. In a typically busy and stressful work environment, a policy manual alone will not prepare people to take the right action. Therefore, create some active learning scenarios that deepen understanding of the impact of day-to-day activity 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 core *Secure.Vigilant.Resilient.* program objectives.

Becoming *secure, vigilant, and resilient* requires that the agency embrace a fundamentally different view of what we've previously called "security." Yesterday's security program was often perceived as a burden — an externally-imposed set of restrictions, rules, and procedural hurdles that impeded business initiatives. Security rigor has been pitted against progress, striking up battles over the budgets and timelines of strategic initiatives. Depending on which prevailed at any given point, the net result has too often been either recklessly risky innovation, or a degree of caution that leads to lost opportunities.

In the pace of today's climate, agencies cannot afford to slow innovation simply because it 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 executives must harmonize these important elements of agency performance through a program to become *secure, vigilant, and resilient*.

Cyber risk and innovation are inextricably linked; rather than subordinating one to the other, senior executives must harmonize these important elements of business performance through a program to become *secure, vigilant, and resilient*.

Contacts

To learn more about how your organization can become *secure, vigilant, and resilient*, please contact:

Deborah Golden
Principal | Federal Cyber Risk Services Leader
Deloitte & Touche LLP
1919 North Lynn St.
Arlington, VA 22209-1742
debgolden@deloitte.com

Gordon Hannah
Principal | Federal Cyber Risk Services
ghannah@deloitte.com

Greg Schmidtetter
Principal | Federal Cyber Risk Services
gschmidtetter@deloitte.com

Chris Goodwin
Principal | Federal Cyber Risk Services
wgoodwin@deloitte.com

Bill Kobel
Principal | Federal Cyber Risk Services
bkobel@deloitte.com

Emily Mossburg
Principal | Federal Cyber Risk Services
emossburg@deloitte.com

Learn more

Federal Practice
http://www.deloitte.com/federal

Cyber Risk Services
http://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html