March 9, 2017 | Ritz-Carlton Pentagon City | Arlington, VA

Federal Executive Briefing

Federal Cybersecurity

PREFACE

On behalf of the Advanced Technology Academic Research Center (ATARC), I am proud to announce the release of this report documenting the Federal Executive Briefing on Federal Cybersecurity held on March 9, 2017, in Arlington, Va.

I would like to take this opportunity to recognize the following session leads for their contributions:

- **Visionary Keynote:** Kenneth Bible, Deputy Director, C4/Deputy Chief Information Officer, Headquarters, U.S. Marine Corps
- **Visionary Keynote:** Rod Turk, Acting CIO/Chief Information Security Officer, U.S. Department of Commerce
- **Panel Discussion:** Col Kevin Seeley, Chief, Infrastructure and Operations Division (J6), Defense Health Agency; David Tillman, Director, Cybersecurity, U.S. Department of Navy; Christopher Wlaschin, Chief Information Security Officer, U.S. Department of Health and Human Services

I also wish to thank the many government attendees who contributed with feedback and their own agency perspectives to our discussion — those contributions certainly enriched the conversation and this report. Among the agencies represented by individual attendees were: Department of Defense/Defense Logistics Agency, Department of Agriculture/Office of Inspector General, DoD/VA Interagency Program Office, Department of Homeland Security/Transportation Security Administration, Department of Homeland Security/Headquarters, U.S. Air Force, Department of Defense/Defense Acquisition University, Department of Health and Human Services/Centers For Disease Control And Prevention/National Center for Health Statistics, Department of Treasury/Internal Revenue Service, General Services Administration, Department of Veterans Affairs, Department of Defense/Defense Health Agency, Small Business Administration, Department of Health and Human Services, Department of Commerce/National Institute of Standards and Technology, U.S. Navy, Department of Agriculture, and the Department of Commerce.

Thank you to everyone who contributed to the ATARC Federal Executive Briefing on Cybersecurity. Without your knowledge and insight, this report would not be possible.

Sincerely,

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)

INTRODUCTION

The one constant about cybersecurity is that it is ever-evolving. Threats, vulnerabilities, data center environments, technologies, responses and strategies — these all continue to morph and require new thinking and approaches.

But it is also important to be mindful that many of the specific features of cybersecurity in federal government environments are quite different than those of commercial environments. Consider, for example, the contrasts between federal and commercial in terms of compliance regimes, business cases, diverse mission imperatives, the consequences and stakes of a breach, bureaucratic decision-making environments, and workforce skills, to name a few.

Federal managers must smartly navigate the fast-changing cybersecurity landscape while also having to address the many specific demands that come with operating within a federal context.

So what strategies, approaches, and capabilities are particularly helpful in achieving good outcomes in this environment?

In March 2017, the Advanced Technology Academic Research Center (ATARC) — in collaboration with BDNA Corporation and marketing partner GovLoop — hosted a "Federal Executive Briefing on Cybersecurity" to discuss how the federal cybersecurity landscape is changing. Roughly two dozen federal cybersecurity executives, specialists, engineers, academics, and other practitioners discussed the specific cybersecurity challenges and approaches that apply to federal civilian agency and Department of Defense environments and where many of today's trends appear to be heading. This report is a summary of those discussions and presentations.

To promote a lively and candid discussion, everything said during the event was considered "not for attribution." Consequently, the substantive points and quotations made during the event and included in this report are not attributed to specific persons.

We have organized this report around two themes that dominated the discussion. The first theme concerns cyber security challenges that federal agencies face; the second concerns approaches and best practices to some of those articulated challenges.

THE CHALLENGES

Broadly speaking, federal cybersecurity challenges tend to fall into three buckets: technical, cultural, and resource challenges.

First, technical challenges — the need to bring automation, data analytics, and other emerging technologies to bear on threats that continue to morph and grow in scale, complexity, and velocity. Second, there are cultural challenges — namely, the need for individuals and organizations to act with greater vigilance, motivation, agility, and effectiveness in reducing enterprise risk in their day-to-day routines. And, finally, there are resource challenges — being able to usher the needed skills, tools, and funds to implement effective risk-mitigation programs. More specifically, these challenges include:

- **Reactive cybersecurity postures.**

  "My office alone spends $100 million a year on cybersecurity and 80 percent of that goes to responding and recovering. It should be 80 percent spent on detecting and preventing."

  Agencies too often play catch-up when it comes to managing their vulnerabilities and mitigating risks. That is because agency IT infrastructures are made vulnerable by end-of-life software and hardware, off-the-books "shadow IT," complexity, and a lack of automation. The result is an inability to smartly (and proactively) prioritize and manage risk in a timely way.

- **Poor visibility into the IT infrastructure.**

  "I think most agencies probably have shadow IT operations that go on — measuring that is a very difficult thing."

  One of the first steps for a Chief Information Security Officer is to take inventory of his or her organization's IT environment. For a large-scale agency — especially one formed through a merger of multiple agencies or bureaus — that's a tall order. Harder still is gaining visibility of unofficial IT assets, known as "shadow IT," that are connected to an enterprise's network by individual employees or off-the-books projects. Many agencies are also unaware of network-connected IT assets that are at or near end of life, unapproved, or out of configuration.

- **Manual, paper-based processes.**

  "Today, we have a lot of people-based management of cyber incidents. Something triggers on the network, a bunch of people pull some data and do some analysis and decide on a response action. That's probably not going to keep up with the adversary — in fact, I can almost guarantee it."

  The sheer scale of federal enterprises and the velocity of cyber threats that afflict them overwhelm manual processes. In some cases, the problem of relying on paper-based processes is linked to bureaucracy and culture. "Whether or not the IG [inspector general's office] will look at [automating the process] favorably is another question," said one participant. "IGs tend to like written pieces of paper and thick binders. That's just the nature of the business."

- **An inability to calculate return on investment (ROI) for cybersecurity investments.**

  "How do you prove or how do you define the value of somebody not infiltrating your network? … [At one of our agencies] we turned away two billion events a week. That's a fantastic metric, but how do I put an ROI on that?"

  Most federal managers struggle with calculating ROI for cybersecurity. Cost figures are available for remediation measures and other direct costs related to cyber security breaches. But, as one speaker said, there are significant intangible costs connected to cybersecurity that are impossible to quantify — things like citizen trust and good will that are eroded when high-profile breaches occur and sensitive information is lost.

- **Insufficient cybersecurity skills among staff.**

  "We struggle to recruit, hire and retain qualified cybersecurity talent. Just in the headquarters alone, we have a 33 percent vacancy rate in our 2210 job series [Information Technology Management Series] for cybersecurity."

  Agencies struggle to compete with the private sector who pay considerably higher salaries for cyber professionals at the same skill level.

- **Limited budget resources.**

  "We recently got a bill on the table. The difference between DIACAP [Department of Defense Information Assurance Certification and Accreditation Process] and RMF [Risk Management Framework] — what program managers are telling me — is a 20 to 30 percent increase over what they were spending on DIACAP."

  Cybersecurity costs money — and budgets are tight and expected to stay that way. Even though cybersecurity is a high priority for most agencies, it is critical that investments are cost-effective, smartly prioritized, and well supported. Moreover, effective cybersecurity is an ongoing investment because the landscape is continually evolving. As one speaker commented: "You also have to fight what I call the completion paradigm … There's no such thing as completion in cyber security."

APPROACHES

Participants noted that there are approaches and initiatives afoot at many agencies that hold promise.

Some can help address the various challenges discussed around change management and culture, skills shortfalls, and transitioning from reactive to proactive cybersecurity postures. Among the approaches discussed:

- **Automation.**

  "Clearly, we have to get to an automated process in cybersecurity so we can get away from those binders and reduce the page count. We're working towards that."

  Automated tools can perform many aspects of cybersecurity: provide visibility of network-connected assets; set and monitor baseline cybersecurity metrics; identify anomalous behaviors that require attention and mitigation; provide situational awareness through dashboards; and enable real-time responses to pre-determined behaviors and actions, among other things. As one participant put it: "Automated tools have come into play and we can now point those at our network and gather more and more data about the number of connected devices and systems that we have."

- **Talk in business language, not IT language.**

  "All I speak about is business outcomes, and I talk to business and mission owners, depending on if they wear a star or a tie. You have to begin to speak in those terms. Once you do that, the argument is easier to make."

  To make a convincing business case for a cybersecurity initiative, talk about risk mitigation and the avoidance of quantifiable impact on business operations and outcomes that support the agency's mission. CFOs and other top agency leaders understand the need to buy down risk and improve value from investments. As one speaker said: "When cybersecurity professionals leave the IT language at the door, and they start talking business language, we begin to resonate with business leaders. For me, I'm saying 'business', and these guys say, 'I own a mission.' Yes, well, it has a business outcome. Even the business outcome of putting rounds on targets — that's the business of DoD. We prosecute and win wars. However, that business outcome has certain inputs." Said another speaker: "We have to get the government into the mindset that cybersecurity is a measurable risk, a measurable outcome, and get into more of a business-like mindset."

- **Compliance is not enough.**

  "It's not enough to measure compliance. The mindset we should have is measuring our adoption of best practices. …. That, I think, is the next step in the measuring of IT."

  Agencies are expected to comply with cybersecurity directives, such as the Federal Information Security Management Act (FISMA). But they will be far more effective if they don't focus too narrowly on compliance and instead focus on how well they are incorporating best industry practices. As one speaker said: "Following a maturity model based on the NIST Cybersecurity Framework, you will get to compliance. But you'll surpass it, in my opinion, by adopting best practices and measuring an IT entity's maturity in adopting best practices. Compliance will come along."

- **Instill cybersecurity into the culture.**

  "Responsibility for cybersecurity is not a CISO game. Cybersecurity is the responsibility of a cybersecurity culture, horizontally and vertically. Everybody has a piece of this. The most important person in a cybersecurity program is the person sitting at the keyboard."

  There are several important pieces to this. Educating everyone throughout the enterprise on how to practice good cyber hygiene is critical. For example, phishing attacks are increasingly sophisticated, so anti-phishing and cyber awareness education campaigns must keep pace. Also, cybersecurity must be embedded into the agency's software development lifecycle (SDLC) from the beginning, such as through agile or DevOps practices. The key is to ensure that cybersecurity thinking and collaboration is a regular part of the software development process from beginning to end. Finally, all members of the agency's top business team must ensure that cybersecurity is accounted for throughout the enterprise. In doing this, it is important for agency leaders to repeat the message that cybersecurity is an all-hands effort and ensure that everyone knows what their role is and what is expected of them. As one speaker said: "This is a second Cold War."

- **Cybersecurity requires a broad set of skills.**

  "The CISO of the future is going to be a renaissance person. It's going to be somebody who not only understands a certain level of the technology, but also has the ability to communicate, write and talk to the executive suite about why they need what they need."

  It's vital that cybersecurity professionals become functionally diverse. They need to understand how technology can help them reduce and mitigate risk, but it is just as important that they be able to understand how they contribute to the broader challenge of enterprise risk management and that they be able to articulate business cases for their priorities.

- **Create and measure to benchmarks.**

  "Figure out what people in your industry or people in your sector are spending for those IT services and measure to that. It'll very quickly show you whether you're paying them too much or have too many people performing that service. But you have to standardize and you have to benchmark."

  It is useful to look at how other comparable organizations — public sector and non-public sector alike — run their IT and cybersecurity operations. What are their costs for various IT service management functions? How many personnel are they using? What is their turn-around time? And what service levels are they delivering? Having such benchmarks enables IT and cybersecurity managers to identify where they need to be, chart a course to get there, and justify that course to their agency's business leaders.

- **Be creative in building a cyber workforce.**

  "My boss developed a workforce development program just for cyber that tries to get folks in early who may not have cyber background at all, but maybe are writers, communicators, business process people, and train them on the cyber skills they need to be effective. And in doing so, in providing that training at different mileposts along their career, reward them with higher salaries, promotions, and, in the long run, hopefully retain them."

  If directly hiring people with cyber skills and experience is too challenging due to competition in the job market, consider developing those employees through training. Training not only helps develop cyber talent organically, it is also a great way to retain employees longer.

- **Reconsider what training is needed.**

  "For too long, training has equaled certification. … We're starting to take a more holistic view of training so it doesn't just equate to the IAM [Information Assurance Management] certification."

  Cybersecurity professionals need to be more well-rounded. They need to understand the bigger picture of how cybersecurity fits into the bigger enterprise risk management picture and be able to articulate the business cases behind cyber initiatives so the agency's business leaders understand it. As one speaker noted: "There has to be more training in the soft skills. I train my folks to be PMPs [Project Management Professionals]. They need to be business minded. If you're not beyond the cyber silo, you've missed it. You partition yourself from the rest of the discussion. We spend too much time in IT for IT's sake. We've got to get to the point where we understand where we sit in risk management."

- **Think about cybersecurity costs differently.**

  "One of the things that I've started to do with some of our projects is identifying it as a sum per fixed cost."

  Applying traditional return-on-investment justifications for cybersecurity investments is challenging — how does one calculate, for example, how many breaches will be blocked by a new piece of software or hardware and the value of those breaches? Viewing cybersecurity more as an integrated function of program cost can work better. For example, at one civilian agency, the cost of the Authorization to Operate (ATO) process is built into the software development life cycle (SDLC).

CONCLUSION

The challenge of protecting sensitive information on federal networks has grown considerably more complex in recent years. This is forcing agency leaders to re-examine how they think about all aspects of the problem, from prioritizing investments and deciding budgets to developing staff and instilling best practices and routines throughout the federal enterprise. Success in cybersecurity can never be viewed in terms of reducing risk to zero, as that is impossible. Rather, it will hinge on each agency's ability to develop proactive, methodical, vigilant and sustainable cybersecurity postures that extend to all members of the enterprise.

ABOUT ATARC

The Advanced Technology Academic Research Center is a 501(c)(3) non-profit organization that provides a collaborative forum for the Federal government, academia and industry to resolve emerging technology challenges.

Founded in 2013 by Tom Suder, ATARC organizes educational events for Federal IT practitioners on topics such as Big Data, Cloud & Data Centers, Cybersecurity, DevOps, Mobile and Internet of Things.

ATARC also introduces innovative technology from research labs to the government and private industry, and provides the government with recommendations for using cutting-edge technology to increase efficiency and reduce cost.