Understanding Federal Cybersecurity Strategies

Best Practices For Agencies In a World of Expanding Risk

Understanding Federal Cybersecurity Strategies

Executive summary

Are you confident in your agency's cybersecurity? Do you think you are detecting and repelling every attack against your network? Are your policies strong, your tools robust and your leaders supportive?

How do you know?

In fact, Federal and Defense agencies are in many cases still stuck in old habits, missing out on the greatest potential of security. You may be among the many who need to rethink their approach to cybersecurity, from planning to acquisition to implementation and beyond.

In this paper, you will learn some of the crucial key strategies that the most forward-thinking Federal and Defense agencies and other organizations use to stay ahead of the ever-changing universe of threats and risks.

The Cisco 2017 Annual Cybersecurity Report documents an information technology environment that is under constant threat from an ever-shifting landscape of attackers, and a cybersecurity posture that still has serious gaps.

In the U.S. Public Sector specifically, organizations often rely on cybersecurity approaches that address specific concerns without fitting into a larger, big-picture view. This might be effective against a particular hack, but it does not contribute to a holistic cybersecurity strategy.

In this paper[1], you will learn:

- Why an enterprise architecture approach to cybersecurity is the best strategic choice;
- The real key to security: it isn't just policies, tools and leaders;
- How the threat landscape is changing, and what is driving the changes;
- How to think about cybersecurity in a new way.

[1] The Cisco 2017 Security Capabilities Benchmark Study, reported and analyzed in the 2017 Annual Cybersecurity Report, was conducted in 2016 across 13 countries with more than 2900 respondents. For this white paper, we will consider only responses from the U.S. Private Sector (433 respondents) and the U.S. Public Sector (59 respondents).

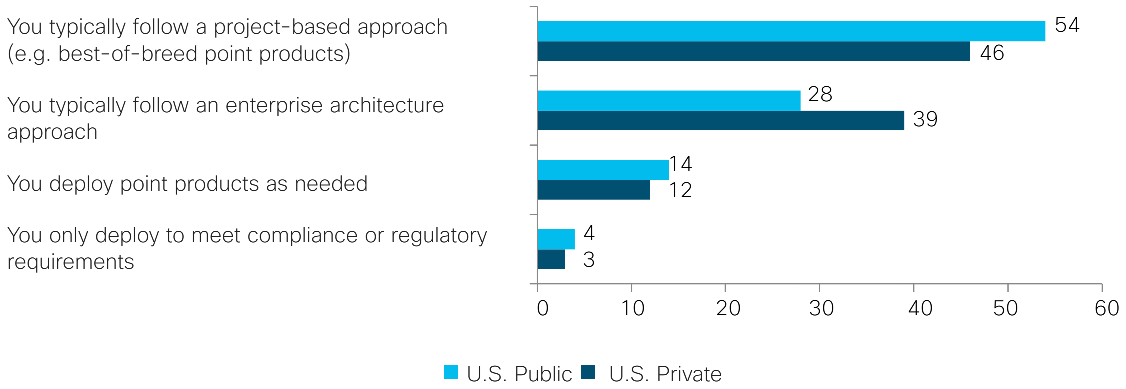
Security architecture

U.S. Public Sector organizations often still rely on cybersecurity strategies that may not be adequate for today's threat environment. U.S. Public Sector organizations are more likely to make cybersecurity purchasing decisions project by project (54 percent), rather than taking an enterprise architecture approach (28 percent).

This best-of-breed approach is usually driven by reaction to attacks, rather than a systematic part of a plan. It usually solves the problem at hand, but it doesn't contribute to an integrated security architecture.

How organizations purchase threat defense solutions

Percent of organizations



You can enhance your protection, then, by simplifying your collection of security tools into an integrated and interconnected security architecture. The integrated tools working together in an automated infrastructure frees up personnel time to address more complex problems. By assessing the security systems you already have, and planning upgrades to fit into an overall strategy – rather than simply reacting to an immediate concern – you can gain the advantages of an architecture without a big capital outlay up front.

An architecture strategy paves the way for systematic, planned expansions that extend the benefits of various cybersecurity products, practices and tools to the entire organization, while preparing you for the next new attack.

For help, you can consult the National Institute of Standards and Technology's Cybersecurity Framework, which lays out best practices and policies.

It is important to understand that the Cybersecurity Framework is only guidance, not a step-by-step roadmap. Organizations must customize it to fit their own individual circumstances. Used correctly, though, it helps you understand, manage and reduce your cybersecurity risks. The Framework help you determine your most urgent needs so that you can intelligently prioritize the investments you make.

NIST now has new tools that allow you to assess your organization against the Framework, and to guide your planning, making it even easier to harness the document's power.

NIST's new Baldrige Cybersecurity Excellence Builder (co-sponsored by Cisco) blends organizational assessment techniques from NIST's Baldrige Performance Excellence Program with the Cybersecurity Framework. Released late in March 2017, the BCEB gives you tools to gauge how effective your cybersecurity efforts are, and to spot opportunities for improvement.

However you approach the opportunity, understand that Federal agencies need a foundational, platform-based approach to cybersecurity. Reacting to the latest data breach to hit the news by hurriedly implementing yet another point solution might feel natural; but as a substitute for a strategy, it leads to a patchwork of solutions from multiple vendors, which ultimately only adds complexity without improving security.

Granted, agencies are hampered by various factors when they try to implement advanced technologies. Money and resource shortages are two big ones.

The top five hurdles to adopting advanced cybersecurity technologies that Public Sector respondents named are:

- Budget (46 percent)
- Current workload too heavy for new projects (29 percent)
- Want to see them proven in the market before buying (27 percent)
- Organizational culture/attitudes about security (27 percent)
- Lack of trained personnel (27 percent)

Attackers find a bigger playing field

Mobile devices, cloud infrastructure and user behavior are all high on the list of worries that security professionals cited in Cisco’s third annual Security Capabilities Benchmark Study. The concerns are reasonable: more mobile devices mean more endpoints to protect. Cloud computing extends the security perimeter. Users are perennially hard to predict and/or train to avoid risky behavior. Federal agencies are carrying out mission-critical activities over their networks, safeguarding sensitive and secret information, and conducting operations that concern the safety and welfare of the nation; keeping those networks safe is their top concern.

But as Federal agencies and other Public Sector organizations embrace digitization and, in the near future, the Internet of Things, the potential attack surface will grow ever larger.

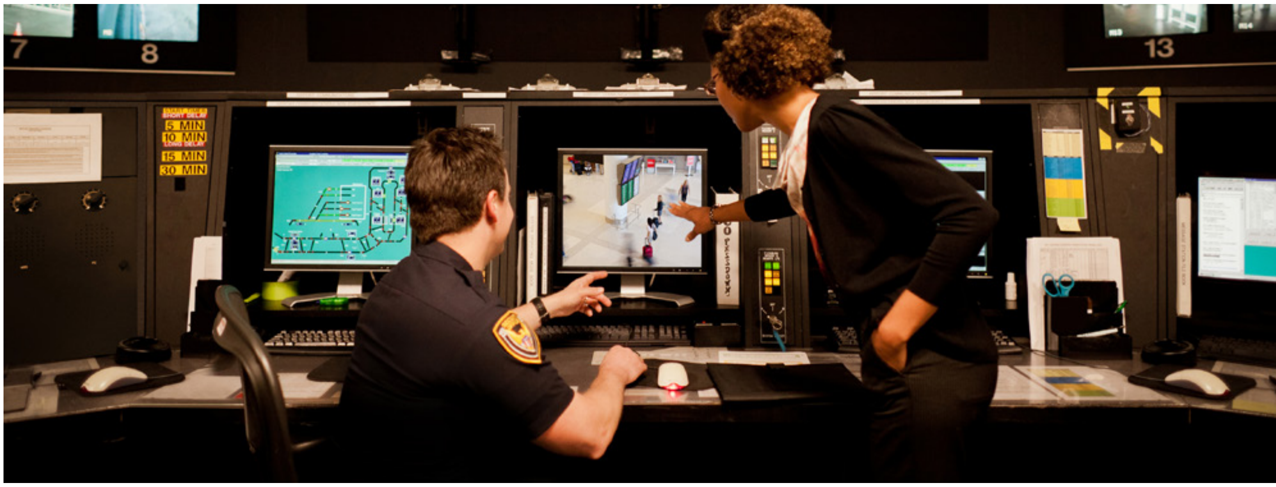
Consider these findings from the most recent Cisco® Visual Networking Index (VNI) report, titled “The Zettabyte Era–Trends and Analysis:”

- Annual global IP traffic will reach 2.3 zettabytes per year by 2020. (A zettabyte is 1000 exabytes, or 1 billion terabytes.) That number represents a threefold increase in global IP traffic from 2015.
- Wireless and mobile devices will account for 66 percent of total IP traffic by 2020.
- From 2015 to 2020, average broadband speeds will nearly double.

Meanwhile, three of the most commonly used exploit kits–Angler, Nuclear, and Neutrino– have vanished, leaving the field wide open for new – and less familiar – tools to take their place. Indeed, new tools are already emerging to fill the gaps that are more sophisticated than their predecessors.

In one sense, this is good news; companies like Cisco who offer powerful security measures from the network’s core to its most remote edge, are making it harder for attackers to succeed, making their work more complex, harder and more expensive. However, that also means the arms race metaphor that has long characterized the continual evolution of safeguards and attacks is going to stay apt for quite some time to come.

Of course, the threat landscape is far bigger than malware scripting kits. Attackers are targeting every possible vector with a wide swath of techniques and strategies, with motives ranging from espionage to simple theft. See the Cisco 2017 Annual Cybersecurity Report for a detailed assessment of the range of threats.

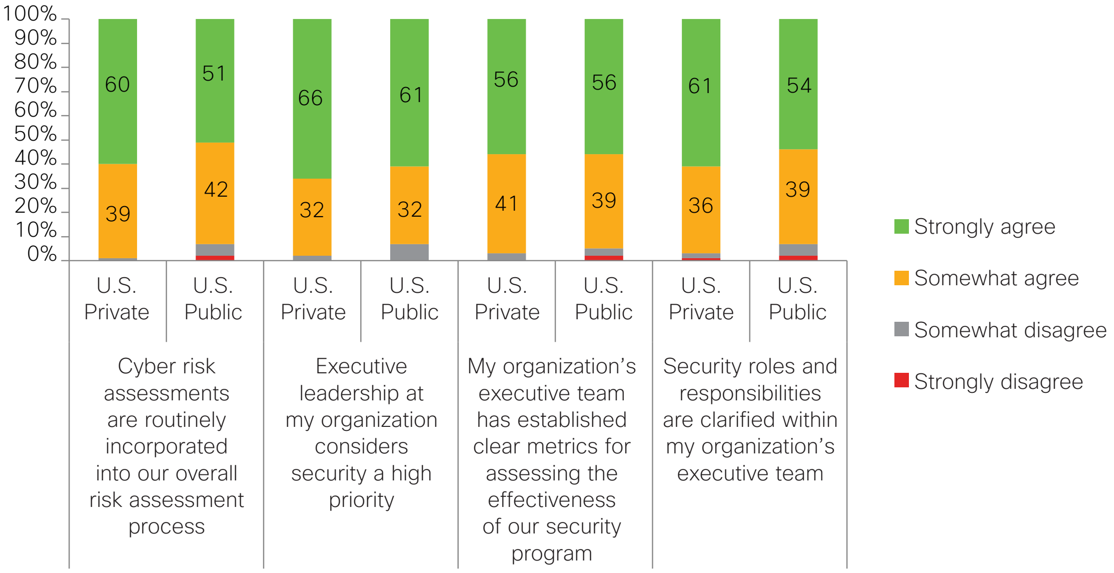


Execution: The key to effective cybersecurity

With the attention brought by recent high-profile data breaches in Federal agencies, leaders in all organizations are feeling a new sense of urgency. Most respondents from U.S. organizations, whether Public- or Private Sector, believe their senior leaders have a good grasp on cyber threats, with the private sector showing a slight edge. The vast majority of respondents agree or strongly agree that their senior leadership teams consider security to be a high priority (98 percent Private Sector, 93 percent Public Sector), and have established clear metrics to evaluate the effectiveness of cybersecurity programs (97 percent to 95 percent).

Opinions of executive leadership

Percent of organizations



Considering only the "strongly agree" responses, both U.S. sectors slightly edge out the global result of 59 percent on the question of whether executive leadership considers security a priority.

U.S. security professionals also trust their tools. Globally, more than two-thirds of security professionals perceive their security tools as very effective or extremely effective. For example, 74 percent believe their tools are very or extremely effective in blocking known security threats, while 71 percent believe their tools are effective at detecting network anomalies and dynamically defending against shifts in adaptive threats.

The U.S. Private Sector boasts even more confidence, while the Public Sector lags slightly. Eighty percent of Private Sector organizations believe their tools are effective or extremely effective at blocking known threats, while only 66 percent of Public Sector organizations do. On the question of detecting network anomalies, those numbers are 77 percent and 69 percent, respectively.

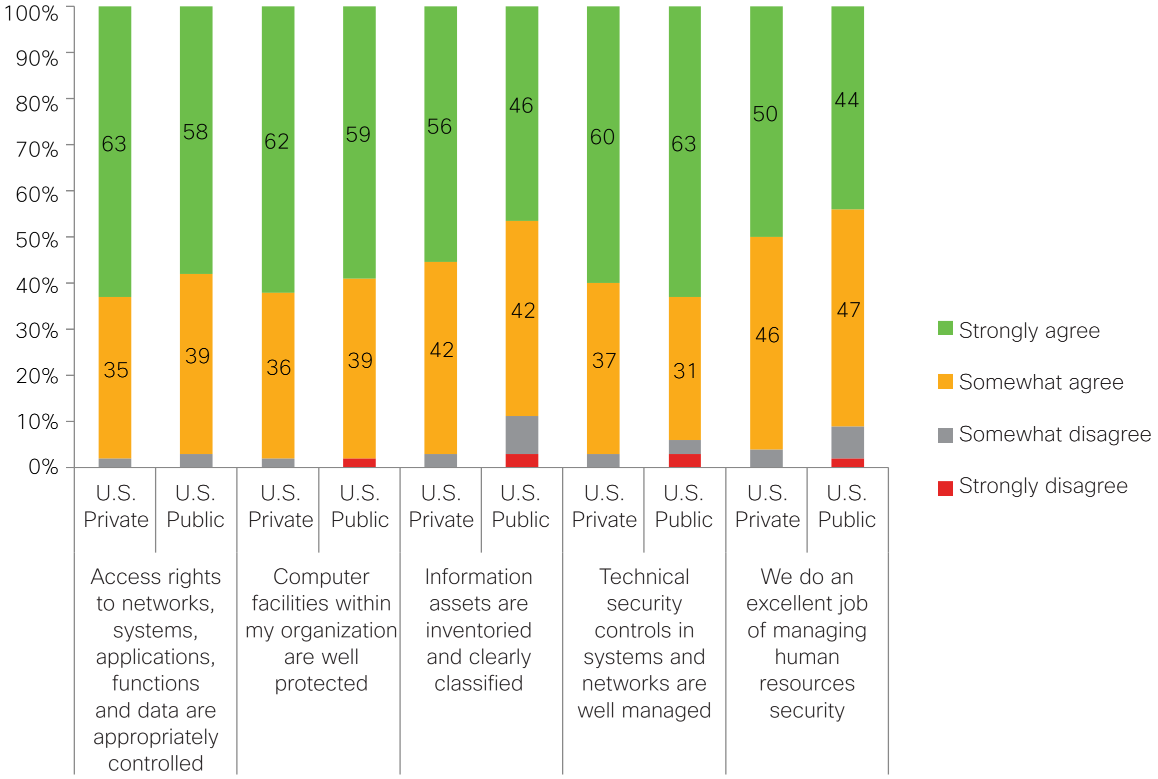
Working hand-in-hand with leadership and cybersecurity tools, policies set the rules for access, use and protection of IT and networks. Again, the majority of U.S. respondents are confident their organizations have set the appropriate policies.

Access control, protection of computer facilities and inventorying of information assets are all part of security policy setting, and in all of those categories and more, almost all respondents in U.S. organizations strongly or somewhat agree their policies are good.

Even the insider threat, which has been recognized as a serious worry for only the past few years, is addressed in human resources policies (such as pre-hire vetting), and in processes for handling employee transfers and departures (to control that employee's access to systems once his or her status changes to one where such access is no longer appropriate).

Opinion of security policies

Percent of organizations



However, while leadership prioritization, strong policies and confidence in the tools are important pieces of the puzzle, they do not in and of themselves guarantee effective security. The master key is execution. No plan can be good enough to overcome poor execution. No policy can be great enough to matter if the organization ignores it in practice.

From policy to effective cyber

Think about it this way: Just what is it that makes cybersecurity programs effective? How would an architecture approach make the difference?

A security architecture shapes an ongoing cybersecurity plan, one which can evolve and adapt as the threat landscape changes, without compromising the larger strategic goal of simplifying and automating security processes to ensure capable execution of policies.

It also simplifies the metrics that you need to chart in order to gauge the effectiveness of your architecture, spot capability gaps and improve performance.

You need to pay attention to two sets of metrics. Operational Incident Metrics show how effective your cybersecurity plan actually is. Time to detection of a breach, and time to remediation of the damage, are common operational metrics.

You also should measure program metrics – implementation of dual-factor authentication, for example, or progress on ongoing modernization projects. Which measures matter will vary from one organization to the next, but tracking them will ensure your execution remains sharp and efficient, and that lapses are found and fixed fast.

Conclusion and recommendations

Today's rapidly expanding attack surface demands an integrated approach to security. An analysis of data from Cisco's Security Capabilities Benchmark Study reveals patterns and decisions that help organizations minimize risk.

Our analysis found several key drivers and several safeguards that characterize organizations with strong security. They are:

Drivers

- **Executive leadership:** The top leadership must prioritize security. This is critical for the mitigation of attacks, as well as their prevention. The executive team should also have clear and established metrics for assessing the effectiveness of a security program.
- **Policy:** Controlling access rights to networks, systems, applications, functions, and data will affect the ability to mitigate damage from security breaches. In addition, policies to ensure a regular review of security practices will help prevent attacks.
- **Protocols:** The right protocols can help prevent and detect breaches, but they also have a strong relationship to mitigation. In particular, regular reviews of connection activity on networks, to ensure that security measures are working, are key to both prevention and mitigation. It's also beneficial to review and improve security practices regularly, formally, and strategically over time.
- **Tools:** The judicious and appropriate application of tools has the strongest relationship with mitigation. With tools in place, users can review and provide feedback that is vital to detection and prevention as well as mitigation.

Safeguards

- **Prevention:** To minimize the impact of security breaches, employees must report security failures and problems. It's also crucial for security processes and procedures to be clear and well understood.
- **Detection:** The best detection methods for minimizing the impact of breaches are those that allow organizations to spot security weaknesses before they become full-blown incidents. To accomplish this, it's vital to have a good system for categorizing incident-related information.
- **Mitigation:** Well-documented processes and procedures for incident response and tracking are key to effective breach mitigation. Organizations also need strong protocols to manage their response to crises.

These drivers and safeguards are mutually interdependent. Security professionals must incorporate all of them in order to seriously attack cyber risk.

Your key goal is to reduce the attack surface available to adversaries, and to quickly detect intruders in the network. It is not possible to stop every attack, but by closing the operational space in which the attackers work, you can make it nearly impossible for attackers to reach critical systems and data undetected.

Learn More

cisco.com/c/en/us/solutions/industries/government/defense-cybersecurity.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**