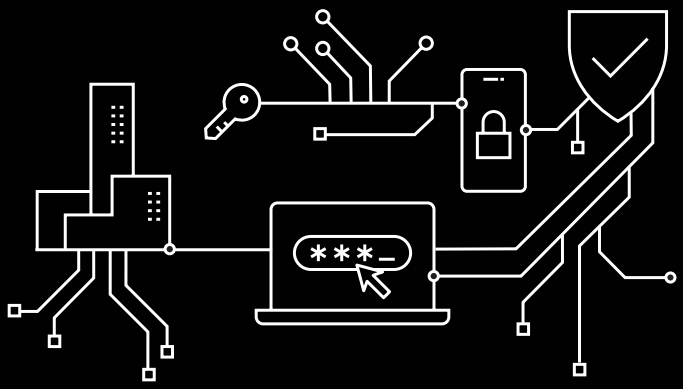
For cybersecurity, strategic outsourcing is a necessity, not a luxury.

White paper

By David Grady
Chief Security Evangelist
Verizon Business Group

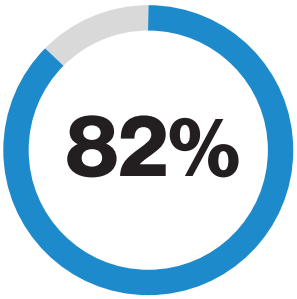


Why read this white paper?

At the same time that organizations of all sizes are exploring the business potential of emerging technologies like the Internet of Things (IoT), 5G and artificial intelligence (AI), cybercriminals are growing more agile and sophisticated. This means that security leaders are under enormous pressure to keep up with "what's next," even as they struggle to keep up with "the basics." A global cybersecurity skills shortage is turning security necessities into security luxuries, and basic security hygiene is suffering. For many under-resourced organizations, strategic outsourcing is the answer.

This white paper is designed to help security leaders demonstrate to stakeholders and decision-makers the value of strategic security outsourcing as their organizations embrace next-generation technologies, and it offers advice on how to evaluate and choose a strategic security partner.

Strategic outsourcing is more than just filling empty seats with warm bodies: It's about partnering with a trusted advisor to take a security program to the next level and about bringing in experts who can support strategic decision-making and help extract maximum value from legacy—and future—security investments.



Eighty-two percent of employers report a shortage of cybersecurity skills.[3]

So much to do, and so little time to do it.

It's rare that an organization claims to have all the cybersecurity resources it needs. And those that do make that claim could be fooling themselves.

Chief information security officers (CISOs), incident analysts, regulatory specialists, deep and dark web hunters, and other cybersecurity subject matter experts are becoming increasingly hard to find and retain. The sheer depth and breadth of cybersecurity domains—Identify, Protect, Detect, Respond, Recover—and the related responsibilities, when contrasted against the lack of available skilled talent, can leave many organizations struggling to protect their IT systems and data.

There are other reasons going it alone with your security program may be increasingly challenging:

- **Good help is hard to find.** CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), reported in November 2019 that the United States faces an anticipated shortfall of almost 500,000 cybersecurity professionals.[1] The White House estimate in May of 2019 was close to 300,000[2]
- **The talent shortage is more than an inconvenience.** A recent Center for Strategic and International Studies survey of IT decision-makers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills. Seventy-one percent believe this talent gap causes direct and measurable damage to their organizations[3]
- **Detecting compromise is taking longer.** When organizations lack the security tools and talent needed to keep "eyes-on-glass" virtually 24/7, cybercriminals are often able to remain in systems longer before the compromise is detected. Verizon's *2019 Data Breach Investigations Report* (DBIR), which analyzed and deconstructed more than 40,000 security incidents and 2,000 data breaches from 2018, showed that most breaches succeed within seconds, but the majority (56%) take "months or longer" to discover[4]

- **Incident readiness plans are neglected.** Maintaining a robust incident response (IR) plan is key to resiliency. But too many security organizations deprioritize maintenance and updates, favoring other activities that can appear more urgent. For the *2019 Incident Preparedness and Response Report*, Verizon found that only 48% of the hundreds of real-world incident plans from 2016 to 2018 they reviewed were "logically constructed" (i.e., adhered to established IR best practices).[5] Only 57% of response plans required periodic rehearsals with stakeholders who have roles in the plan. When IR becomes "we'll get to it," it probably won't be gotten to until a crisis strikes
- **Cyber "blind spots" flourish in underskilled organizations.** Thirty-four percent of incidents and breaches examined in the 2019 Verizon DBIR were traced back to insiders—employees and third parties with access to corporate systems and data who did bad things, either intentionally or unintentionally.[4] In overburdened security programs, third-party risk assessments may be limited to questionnaires, with comprehensive site visits of critical suppliers a rarity. Properly combatting insider threats means thoroughly reviewing business processes that can lead to data leakage, and having the skills to develop and deploy controls that protect data without creating bottlenecks

In overburdened, understaffed organizations:

- Vulnerabilities may go unidentified and unpatched for dangerous lengths of time
- Third-party vendor oversight is limited to perfunctory questionnaires, resulting in a "trust, but don't verify" assurance program
- Threat intelligence remains a firehose of information, difficult to operationalize and optimize
- Untuned SIEM systems create more noise than signal, resulting in chronic "alert fatigue"
- Business-enabling technologies like mobility, cloud and IoT don't get the security scrutiny they require

Maintaining collaborative relationships with business-unit leaders outside of IT is often seen as a burden. As a result, IT-driven business innovation can suffer, and operating risks increase. Security should be established as a cornerstone of the organization from the start.

Organizations struggling to manage cybersecurity in-house should seriously consider outsourcing. A strategic security partner can help organizations establish end-to-end program visibility while also filling in critical cybersecurity gaps. These gaps may range from operational (penetration testing and patching) to transformative security information and event management (SIEM) optimization, AI and security orchestration automation. The right partner can help transform security from an organizational liability into a business enabler.

The case for strategic outsourcing

There are multitudes of cybersecurity vendors offering "[fill in the blank] specialty as a service." But as threats grow and digital transformation sweeps through industries, security leaders must reevaluate their approach to outsourcing. Tactical outsourcing—that is, bringing in contractors to fill seats and enable the latest spot solution—will not help transform a security program. Or the organization.

Strategic outsourcing, or "co-sourcing," on the other hand, enables security leaders to evaluate where a program stands, determine where it needs to go, plot a course for how to get there and take the necessary steps. Done right, strategic outsourcing can lead to a partnership where the outside security provider becomes a trusted advisor, and cybersecurity is viewed by organizational leadership as a corporate asset rather than a cost center.

Strategic outsourcing helps security leaders reflect on their mission and priorities and determine if their team has the right mix of skills to accomplish well-defined program goals. Faced with digital transformation and next-generation security challenges, such as cloud and mobile attack vectors, CISOs must ask themselves:

A. Is our team better equipped to handle day-to-day operational security fundamentals, or to evaluate and implement next-generation security technologies?

B. Should we consider outsourcing operational program elements like day-to-day security monitoring so we can focus our in-house team on other priorities?

C. Or are we somewhere in between A and B, and need help in both areas?

How you choose to utilize a partner and design your joint Responsible, Accountable, Consulted and Informed (RACI) matrix is a strategic decision in and of itself. Outsourcing with the right partner allows security leaders to take an honest look at their programs, identify and fill gaps and extract maximum value from security technology investments. The right partner knows how to meet you where you are on your security journey, and rarely recommends "rip and replace" as a strategy.

The right partner-provider will also help you plan for the future by providing subject matter expertise in emerging technologies and security techniques, as well as emerging threats. This is the kind of mastery that many security leaders struggle to find time to develop and maintain, given the pressures of day-to-day security demands.

Choosing your strategic security partner

The following are some tips to help you evaluate potential security partners:

- **Engage key stakeholders.** Internal stakeholder engagement is a critical first step in making the case for strategic outsourcing. By engaging stakeholders inside and outside of IT, and by educating them about the benefits of strategic outsourcing, the CISO and their team can create a coalition of influencers and allies. No one should think that outsourcing is an admission of program failure. If a CISO can tie the use of a strategic security partner to business objectives and show how security can enable new business models and enhance the customer experience, they will foster a more positive perception of the security function across the enterprise
- **Engage current security staff.** If current staff isn't consulted about the objectives of strategic outsourcing, they could feel threatened. In reality, security staffers will benefit from their interactions with, and exposure to, the right provider's subject matter experts and industry experience. Including them in the entire process, from partner evaluation to RACI design, may result in a more engaged and satisfied security team
- **Analyze the analyst reports.** Narrow the list of potential partners by looking at analyst reports—and read the details. Most of the major firms (Gartner, IDC, Ovum, ESG, etc.) evaluate managed security services (MSS) providers, and their reports should help inform the strategy behind your outsourcing effort
- **Ask tough questions.** Require that potential strategic security partners demonstrate solid experience in securing complex environments, as well as expertise in emerging security tools and techniques. For example:
  - How did the provider help a company expand its IoT program by using security as a program driver?
  - How did it help an organization accelerate compromise detection by using autonomous threat hunting and AI tools?
  - Can the provider demonstrate its expertise in dark web hunting, or SIEM platform management and optimization?
  - Has it helped other organizations tackle complex regulatory challenges like the General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA)?
  - Can the provider explain how it works effectively alongside other ecosystem partners to minimize the need for costly "rip and replace" efforts?
  - Does the potential partner have a proven and documented methodology for integrating capabilities and people into an existing security operation?
  - And does it have established processes for driving continuous service improvement for the life of the contract?
- **Leverage proven industry frameworks.** ITIL and COBIT 5 provide comprehensive methodologies for evaluating and selecting strategic vendors
- **Be judgmental. Are you compatible?** All the award-winning security capabilities in the world won't matter if you and the providers' team don't jell. As with any long-term relationship, chemistry matters. As do effort, trust and honest communication

Building a stronger internal team

To address the cybersecurity staffing shortage, Forrester Research advises that organizations redefine what makes a good security candidate. Rather than hiring only those with security certifications, consider motivated individuals with other applicable skills: military or law enforcement experience, accounting, IT and/or network management, strong written and oral presentation skills, and the ability to think outside the box. Then teach them security.

Security leaders should consider growing or revitalizing their own teams in parallel to strategic outsourcing to create a more dynamic, responsive and flexible cybersecurity environment. The stakes are too high, and the threat landscape is evolving too quickly, to simply maintain the status quo.

Learn more:

To learn how Verizon partners with enterprises to help protect against today's cyberthreats and prepare for what's next, visit https://enterprise.verizon.com/products/security/

Or request a consultation: 877.297.7816

1 https://www.isc2.org/Research/Workforce-Study
2 http://www.dhs.gov/news/2019/05/02/white-house-cybersecurity-workforce-executive-order-bolsters-us-frontline-defenses
3 https://www.csis.org/analysis/cybersecurity-workforce-gap
4 enterprise.verizon.com/resources/reports/dbir/
5 enterprise.verizon.com/resources/reports/vipr/

verizon