WHITE PAPER

The Bedrock of IT Security Starts with Training

Jim Zimmermann
Director, Solutions Practice,
Skillsoft

skillsoft

EXECUTIVE SUMMARY

As companies embrace mobile applications, cloud computing, and other high-value innovations, new and larger vulnerabilities have emerged. Now uninformed, careless, or disgruntled employees can create profound security disruptions. While information security is everyone's job, it is the IT experts who bear the greatest burden. As hiring skilled security talent becomes more challenging, many organizations are investing in comprehensive training programs to shore up skills, lower HR costs, and improve the continuity and consistency of their security initiatives. This white paper outlines the many training initiatives that organizations can pursue to improve security.

A FAST-CHANGING LANDSCAPE FOR CORPORATE IT SECURITY

Mobile platforms, big data and cloud-based architectures are creating significant challenges and demands for the entire IT ecosystem. The issue that now dominates the corporate agenda is IT security—and rightfully so. According to the 2018 Global State of Information Security Survey (GSISS), "59% of security leaders say digitization has increased information security spending."[1]

Even the most careful organization is vulnerable. A smartphone or laptop inadvertently left in a cab or a well-intentioned lending of access privileges to an unauthorized user can open the door to far-reaching consequences. Despite organizational efforts at ensuring employee compliance, PwC found that most security incidents stem from current employees.[2] While it now means that IT security is everyone's job, it's clear that the most important role is played by the IT experts: the people who understand the issues and nuances of securing an organization's most valuable assets. Unfortunately, these talented professionals are in short supply and high demand.

THE IT TALENT CRISIS

For years, corporations viewed their IT departments as cost centers and steadily outsourced many of their IT functions to exploit favorable economics. This resulted in the IT industry shedding both thousands of jobs and large amounts of brain power.

However, companies are now identifying their IT services and functions as a rich source of differentiation, innovation and competitive advantage: the exact areas that outsourced IT resources have trouble addressing and improving.

Seeking to jumpstart their efforts to strengthen security, organizations are once again scrambling to hire talented technologists. But today, the search for top talent in IT is has far progressed past being just an inconvenience and now constitutes a significant business problem.[3]Many large organizations are looking to hire thousands of new IT professionals in a job market where IT unemployment is at historic lows.

1 "2018 Global State of Information Security Survey." IDG, December 8, 2017.
2 "The Global State of Information Security® Survey 2018." PwC, CIO and CSO, October 18, 2017.
3 "7 IT Salary and Hiring Trends for 2018." Sarah K. White, CIO, November 2, 2017

The hiring challenge is especially acute in cybersecurity. Salaries for newly minted college IT security graduates are starting at more than $100,000, while freelancers and contractors are commanding hundreds of dollars per hour for their services.

70% of cybersecurity professionals say the cybersecurity skills shortage has had an impact on their organization.[4]

"67% of cybersecurity professionals claim they are to busy with their jobs to keep up with skills development and training."[5]

51% of organizations claim to have a problematic shortage of cybersecurity skills.[6]

Talent shortages are estimated to reach 1.8 million professionals in cyber security by 2022.[7]

INCREASING THE TALENT OF YOUR CURRENT TEAM

In the face of this critical shortage of IT security talent, many organizations have decided to take their existing team's security skills to higher levels of expertise with training. Training's value to an IT organization is well known, but often not appreciated for all it can do to help mitigate talent shortages.

4 "Cybersecurity skills shortage creating, recruitment chaos." John Oltsik, CSO, Novemeber 28,2017.
5 "Cybersecurity professionals aren't keeping up with training." John Oltsik, CSO, December 5, 2017.
6 "Cybersecurity Job Fatigue." John Oltsik, ESG, February 6, 2018.
7 "2017 Global Information Security Workforce Study, Benchmarking Workforce Capacity and Respinse to Cyber Risk." Frost & Sullivan, Center For Cyber Safety and Education, 2017.

Security professionals know that stale or outdated skills are disastrous for their careers. When employees see that they aren't being offered the resources they need to keep their skills up-to-date, they are much more likely to seek employment somewhere else where they will get the training they need. By using training to help retain your current staff, you not only avoid the time, cost, and the headache of replacing scarce resources, you also keep the institutional memory of the subtleties and nuances regarding how IT is executed in your organization. This provides a highly desirable level of continuity and consistency across your organization.[4]

On-going training that helps up-skill and re-skill existing IT employees is no longer an option but a necessary pillar for retention in any successful organization.

IT and cybersecurity leaders need to look at training as a tool to help retain, attract, reward and re-skill staff.

The competition for new security talent is intense. In North America, 68% of industry professionals report there are too few cybersecurity workers in their organization and most believe it's because there aren't enough qualified candidates.[8] Many companies do not have the big budgets to offer fancy perks to attract talent to their organization, but they fail to realize that the training they offer their staff is highly valued by top talent. Millennials are soon to surpass baby boomers as the largest living generation and value training more than any other group, with over half of millennials saying organizational training was "very important."[9]

And although offering training as a tool to re-skill existing employees is generally appreciated, it is often mistakenly viewed as a tool only to re-skill your current staff.

Don't forget about the many employees outside of IT in your company when you are looking for talent. Having a plan to re-skill non-IT staff to assume entry-level jobs in IT is a sound long-term strategy to address ongoing talent shortages—talent shortages are estimated to reach 1.8 million professionals in cyber security by 2022.[10]

8 "2017 Global Information Security Workforce Study, Benchmarking Workforce Capacity and Response to Cyber Risk." Frost & Sullivan, Center For Cyber Safety and Education, 2017.

9 "Meet the Millennials, The Next Generation of Your Information Security Workforce." Frost & Sullivan, Center for Cyber Safety and Education, 2017.

10 "2017 Global Information Security Workforce Study, Benchmarking Workforce Capacity and Response to Cyber Risk." Frost & Sullivan, Center For Cyber Safety and Education, 2017.

THE VALUE OF CERTIFICATIONS

Security-related certifications should also be a key part of any security training programs. Certifications can reduce risks by helping employees stay on top of the changing IT security landscape while validating their skills and knowledge. These certifications help ensure employees are competent in assessing, mitigating, responding, monitoring and reporting security risks and breaches.11[11] Plus, if your organization does suffer a breach, authorities will often look at the training and certifications that your staff received. If you can show that you made the effort to train and certify staff to keep your company's data and infrastructure safe, you will be much better prepared to defend yourself in the event of lawsuits or penalties arising from the breach.

WHAT TODAY'S IT LEARNERS WANT AND NEED

Today the IT learner wants:

- **Expert-led instruction:** Authenticity and credibility matter—especially for critical topics like IT security. Learners want to hear from engaging subject-matter experts, not paid actors or professional voiceover talent.

- **Multiple types of learning:** One size does not fit all for training. Today's security professionals want, and need, different types of learning for different needs. Type of learning that is in-demand today includes self-paced courses, videos, eBooks, live practice environments, mentoring and boot camps.

- **Hands-on learning:** Learners report that they value the content of videos, classes and books—but they want to put those lessons to work with practical application. Hands-on learning creates excellent retention and is a learning style that has particular appeal to IT pros.

- **Brevity:** No matter the content or modality, there's one thing virtually all learners agree on—short, targeted learning resources that align with their goals and their current (often urgent) needs. Even if a complex topic requires several hours to learn, most learners prefer to consume the training in short bite-sized portions that can fit into and around their busy schedules.

11 "The 13 Most Valuable IT Certifications Today." Sarah K. White, CIO, January 31, 2018

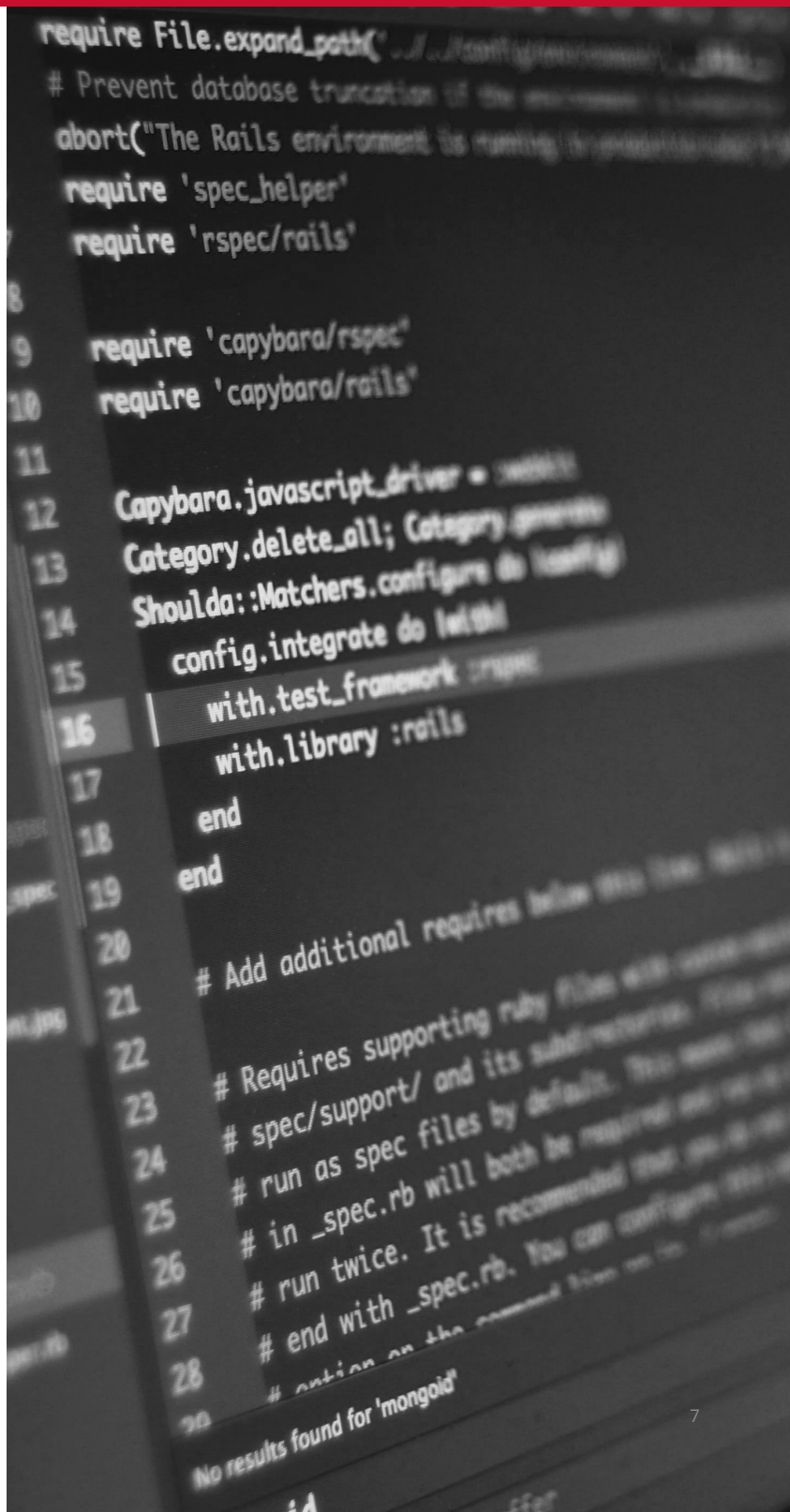
- **Ease of access:** Security professionals do not have the time or patience to jump through hoops to find the learning resources they need, when and where they need them. It is important to make sure resources are easy to access and find. Content must be available on any device desktop, laptop, smartphone or tablet and at any time or location.

THE PURSUIT OF CONTINUOUS LEARNING

The IT domain—and security, in particular—is a discipline that requires a commitment to continuous learning. The issues, innovations, threats and underlying technologies are all in a constant state of change, which means your organization must dedicate the time and resources to stay abreast of new developments. In this ever evolving environment, event-based, episodic training can't keep pace, and just taking courses isn't enough.

Most IT leaders and staff, however, have technical backgrounds and have little business skills training or experience. Team members may have been recruited from outside the company and have limited knowledge of the organization or its issues, overall strategies or goals. IT teams often struggle to provide a basic level of business, communication, business analysis, project management, management, leadership and other "non-technical" skills to their teams.

This is what makes collaboration with other business units, as well as strategic hiring and training practices, of the utmost importance. If CIOs don't put time and resources into establishing relationships with leaders and teams outside of IT, they will find themselves marginalized and compartmentalized. Business units have many cloud-based service offerings that they can use to "build their own solutions" without IT's help, so IT needs to get ahead of the curve and seek out relationships through the company. And CIOs cannot afford to neglect their relationships to the rest of the C-suite and other senior executives and to help them understand the value that IT can bring to their organizations.



HOW SKILLSOFT CAN HELP

Skillsoft is the leading provider of IT security training. We are the choice for everyone from advanced IT security practitioners to security "awareness" training for people outside of IT. Unlike other providers who only focus on one "type" of IT Security training (like video based or instructor led), Skillsoft offers a wide array of learning types that can be easily assembled into a comprehensive curriculum to meet the needs of specific groups of learners. Skillsoft offers self-paced subject matter expert-led courses, performance support videos, fully searchable online books from leading publishers, assessments and exams, virtual instructor-led training and access to skilled mentors. Skillsoft is also the leading certification training company and supports over 100 IT and business-related certifications including beginner, intermediate, advanced, and expert security certifications.

ADDRESSING IT SECURITY AT YOUR ORGANIZATION

Security is the number one IT priority. But the scarcity of security-savvy IT pros means many companies are, through sophisticated education and training strategies that reward and retain employees, investing in their own people, while improving corporate security.

From expert-led instruction and quick, on-demand videos to continuous hands-on experiential learning, organizations are putting in place complete frameworks for training and certification that will tighten corporate IT security and make them less vulnerable. Visit Skillsoft's page on cybersecurity for resources and more information on how to keep your organization secure.

ABOUT THE AUTHOR

Jim Zimmermann is the Director of Skillsoft's Solution Practice and the practicing Solution Principal for IT and Digital training solutions for North America and EMEA. Jim holds a BS in Natural Sciences from St. Thomas Aquinas College and leads a team of Solution Principals that support all of Skillsoft's core training coverage areas including business and management, leadership development, IT and digital and compliance.

During his 40+ years in the IT and media industries, Jim has worked for the largest IT firms as well as SMBs and startups. Jim started his career as a scientific programmer for an environmental engineering firm where he ended up teaching programming to other scientists. Jim went on to hold positions in product management, product and corporate marketing and technical consulting.

For more than 15 years, Jim has worked for Skillsoft in a variety of capacities, starting in the Books business where he created the AnalystPerspectives collection, moving to directing the Product Marketing efforts for Skillsoft's entire award winning IT and Digital Skills training product line. In his current role, he works with Skillsoft's largest strategic customers to help them provide optimized solutions for training their leaders, managers and staff.

Jim Zimmermann

Director, Solutions Practice, Skillsoft

linkedin.com/in/jim-zimmermann-4a2736

@jimlzim

skillsoft

linkedin.com/company/skillsoft

facebook.com/skillsoft

twitter.com/skillsoft

skillsoft.com

US 866-757-3177
EMEA +44 (0)1276 401994
ASIA +65 6866 3789 (Singapore)
AU +61 2 8067 8663
FR +33 (0)1 83 64 04 10
DE +49 211 5407 0191
IN +91-22-44764695
NZ +64 (0)21 655032

ABOUT SKILLSOFT

Skillsoft is the global leader in corporate learning, delivering beautiful technology and engaging content that drives business impact for modern enterprises. Skillsoft comprises three award-winning solutions that support learning, performance and success: Skillsoft learning content, the Percipio intelligent learning platform and the SumTotal suite for Human Capital Management.

Skillsoft provides the most comprehensive selection of cloud-based corporate learning content, including courses, videos, books and other resources on Business and Management Skills, Leadership Development, Digital Transformation, IT Skills and Certification Training, Productivity and Collaboration Tools and Compliance. Percipio's intuitive design engages modern learners and its consumer-led experience accelerates learning. The SumTotal suite features four key components built on a unified platform: Learning Management, Talent Management, Talent Acquisition and Workforce Management.

Skillsoft is trusted by thousands of the world's leading organizations, including 65 percent of the Fortune 500. Learn more at **www.skillsoft.com**