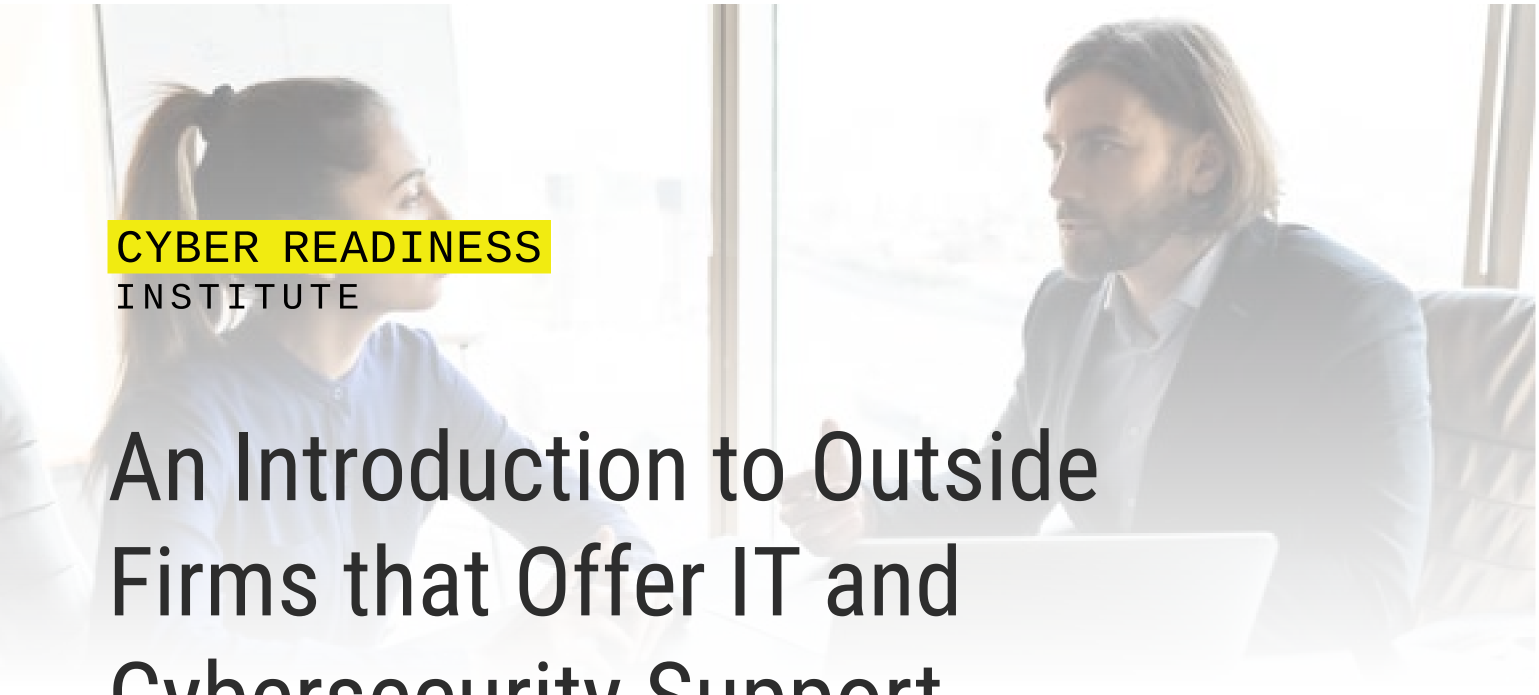

CYBER READINESS
INSTITUTE

An Introduction to Outside Firms that Offer IT and Cybersecurity Support

Second in a series on using outside firms to reduce your cybersecurity risk.

Like many small businesses, you've come to the conclusion that you need outside information technology (IT) and cybersecurity support. Maybe you've been hearing about more cybersecurity breaches in the news. Maybe you know a company that had a ransomware attack. If you still are not sure whether you need help, take a look at the **first guide** in this series, "Should I Get Outside Support for Managing My Cybersecurity Risk?"

You realize that IT and cybersecurity are becoming business management "fundamentals" – like finance and sales. But you don't have the time to figure it all out. If you're like most small business owners or managers, you may not be sure what kind of support you need or even what questions to ask. This series from the Cyber Readiness Institute's Small Business Advisory Council will help guide you through the process of determining if you need outside help and how to get the help you need.

Always remember that ultimately, you are responsible for the cyber readiness of your organization. You can outsource certain functions, like installing software updates, but you are accountable for setting the policies, building a cyber ready culture, and satisfying any privacy and security compliance obligations.

As the threat of cyber attacks has escalated, so have the number and types of companies offering their assistance. It is a confusing market with overlapping service offerings and more acronyms than you can imagine.

One of the first decisions is whether you want to hire a trusted IT/cyber advisor to guide you through the process or wade through the vendors on your own. We know that the idea of hiring a consultant to pick the right vendor(s) can seem like an added expense. However, it may be less expensive in the long run because they can ensure that you are getting the services you need at a fair price. Ultimately, you need to determine who to trust in order to get the help you need.

Here is a list of the **types of companies** you'll encounter and a brief description. Remember there will be some overlap in the types of service they provide. The next guide in the series will discuss how to select the right level of outside support.

IT Consultant

Analogous to an IT handyman. Generally speaking, the IT Consultant helps prevent problems from occurring and fixes problems that do occur. They assist with setting up your network and/or WiFi, building and maintaining websites, recommending and installing software, setting up emails, setting up user accounts, creating and testing backups, and more.

Managed Service Provider (MSP)

MSPs are typically small firms that offer similar services to IT consultants. They often are certified installers or advisors of several hardware and software vendors. Some boutique MSPs say they specialize in cybersecurity, meaning their services would overlap to a greater extent with those of an MSSP.

Managed Security Services Provider (MSSP)

The MSSP will verify that the MSP is building and maintaining the network to maximize value and reduce risk since some MSPs and IT consultants have limited knowledge about cybersecurity technology or monitoring. MSSPs often perform activities like intrusion mapping, log checking, technology risk assessment, planning and consulting, compliance with policies, procedure development, user support, proactive security response, monitoring, and incident response.

Virtual Chief Information Officer (vCIO)

For businesses that may need a CIO within their workforce, vCIOs offer a way for you to outsource the function, similar to how you might outsource General Counsel or Chief Financial Officer functions. This approach tends to be for companies that are a little larger on the small to mid-size scale. vCIOs will manage, implement, and recommend products and services to improve your IT and security levels.

Here's a list of the **most common and respected types of certifications** or professional credentials you may encounter when assessing those who provide outside support.

General cybersecurity credentials:

CISSP – Certified Information Systems Security Professional

- This is a broad, yet advanced certification that is widely applicable as it is not vendor-specific. It requires 5 years of experience to pursue it.

CISM – Certified Information Security Manager

- This requires 5 years of experience to pursue it and is very advanced. Those who who have obtained this credential typically manage security at the organizational level (e.g., CISOs).

CompTIA Security+

- A basic certification that provides a good basis to build on with other more advanced credentials.

Specialized credentials (depending on need):

SANS

- SANS offers a variety of technical certifications, divided into focus areas such as Cloud Security, Penetration Testing and Ethical Hacking, and Security Management, Legal and Audit.
- The SANS GIAC Security Essentials (GSEC) certification strikes a good balance of signaling that the credential-holder has a foundation of broadly applicable knowledge, as well as specific, technical skills.

CISA – Certified Information Security Auditor

- As the name suggests, this credential is intended for roles focused on auditing and compliance.

CIPP – Certified Information Privacy Professional

- This credential focuses on data privacy as it relates to legal and regulatory matters.

CEH – Certified Ethical Hacker

- This credential means the individual has learned how to think like a hacker, but use those skills to protect and prevent attacks, as opposed to penetrating a system with malicious intent.

This guide has provided information on the types of organizations and credentials you may encounter. If you're now asking yourself how to select the right type of outside support for your business, look for our next guide in this series, **"How to Select the Right Level of Outside Support."**

The complete list of guides in this series:

Should I Get Outside Support to Manage My Cybersecurity Risk?

Introduction to the Types of Outside IT and Cybersecurity Support

(THIS GUIDE)

How to Select the Right Level of Outside Support

Reviewing and Understanding the Contract

Your Ongoing Cybersecurity Responsibilities

Contributing Authors

Special Thanks

- Marc Pillon, IT Ally
- Brian Kelly, EDUCAUSE
- Dawn Yankeelov, TALK
- Faye Francy, Auto-ISAC
- Ilene Klein, Cybercrime Support Network
- Jill Tokuda, CyberHawaii
- John Bryk, DNG-ISAC
- Michael Pritchard, Netchex
- Tanya Bolden, AIAG
- Walter Bran, ICC Guatemala
- Stan Stahl, SecureTheVillage

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.