COVID-19 Cyber bulletin

27 April 2020

Patch up, ramp up, back up — consider Cybersecurity Managed Services

This bulletin is designed to help you consider managed service options as you navigate the increased cyber risk profile caused by the new work-from-home (WFH) world. This is week six of shelter-in-place for many companies, and by now most organizations have settled into a new type of normal. While social distancing is likely to remain in effect for some time, companies are starting to talk actively about back-to-work plans. In some cases, information security (InfoSec) resources may not return to their previous roles, as they have been reallocated to new priorities, such as monitoring remote workers and videoconferencing. Some functions or projects may continue to be effectively performed remotely, although they were once considered on-prem only. As we work through the pandemic, most InfoSec teams will encounter budget cuts, workforce rightsizing, and a backlog of work to manage security events and to meet 2020 goals and regulatory commitments. It is a good time to think about a revised 2020 cybersecurity strategy and road map. Exploring managed services, in the form of an outsourcing or cosourcing model, may be a quick and effective way for you to overcome these hurdles, maintain traction with your 2020 commitments, and provide scalability and workforce flexibility.

Cybersecurity is increasingly diverse and complex and is now a critical function to enterprise risk management requiring constant proper due care. The COVID-19 pandemic has demonstrated the negative impact of rapid operational disruption. The need to temporarily redirect internal resources, surge in certain areas or obtain specialized resources can make adding an outsourcing partner to your strategy a sound component to your business risk management efforts. At minimum, seeking help with critical cybersecurity operational functions, such as cyber threat detection and response or identity and access management might be the right decision.

Benefits of managed services Include:

- Cost efficiency – high levels of protection can be obtained without the investment in staff and infrastructure
- Access to dedicated security professionals with up-to-date understanding of threat actor tactics, techniques and procedures, and the latest threat detection and incident response measures
- 24/7 real-time monitoring, analysis and protection without the cost of hiring, training and retaining in-house resources
- Workforce flexibility/scalability and the ability to quickly fill skills gaps (even those unique specialist skills that are expensive to retain and are not deployed full time)
- Acceleration in the maturity of capability, including leveraging automation
- Outside perspective on your security posture, including best-in-class standards
- Freeing up of in-house resources for other matters, which may include periodically fighting fires in impactful areas
- Increased resiliency by allowing certain functions to be delivered off-prem
- Proven repeatable processes and procedures; clearly defined service level agreements (SLAs) to maintain quality
- Application of lessons learned from other sectors and organizations to drive continuous improvement and promote innovation

The most common reasons cited for not moving to a managed service model are concerns over loss of control and atrophy of capability. However, the speed of deployment and the ability to accelerate and sustain capability improvements with a reliable and consistent service make managed services an option worth considering. The best managed services providers emphasize a teaming and consultative approach that focuses on maturing your capabilities, adding integration and going beyond the achievement of SLAs and other traditional key performance indicators.

When considering a managed services provider, look for:

- A trusted advisor known for excellence in the broadest range of cybersecurity skills and capabilities who knows your business
- A flexible provider that can support a specific project or function, as well as an entire set of needs and services
- A delivery approach that integrates into your operations and helps you become more efficient and cost-effective
- A project manager that accepts ownership and communicates operational outcomes in a way that is timely and relevant to the business and that resonates with the Board of Directors and audit committee
- A partner focused on helping you elevate/mature your cybersecurity capabilities as an extension of your team over time through innovation, workflow automation, orchestration and remediation

EY Cybersecurity contacts:

Steve Ingram
EY Americas Financial Services and BCM Cybersecurity Leader
steve.ingram@ey.com

Chris Mikucki
EY Americas Cybersecurity Resilience Leader
chris.mikucki@ey.com

Matt Hynes
EY Americas FSO Insurance Cybersecurity Leader
matt.hynes@ey.com

Angela Saverice-Rohan
EY Americas US Privacy Leader
angela.savericerohan@ey.com

Natasha Wheatley
EY Americas FSO WAM Cybersecurity Leader
natasha.wheatley@ey.com

Christian Torres
EY Americas FSO Client Cybersecurity Executive
christian.a.torres@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYGM Number 002529-20Gbl
ED NONE

ey.com