ENTERPRISE
INTEGRATION

VIRTUAL CISO
AN ECONOMICAL EXTENSION

DESIGNED TO PROVIDE EXPERT SECURITY INSIGHT, LEADERSHIP AND SUPPORT

Enterprise Integration | entint.com | 888-848-9332 | info@entint.com

Information Security risk has long been a central concern for nearly every sector of the economy. Not a week goes by without headlines about another data breach. Cyber attacks can now happen in hours instead of days or weeks. Cybercriminals are collaborating with another and becoming increasingly more sophisticated in their attacks. How you handle and protect your data is vital to the security of your business and the privacy expectations of your customers and employees.

Have you selected a cyber-security framework?

Y N

Do you view cyber security in terms of Risk as opposed to a set of controls implemented by our IT department?

Y N

Are you protected against vulnerabilities on your networks?

Y N

In the event of a breach, can you quickly determine impact, contain the breach, and respond to the incident (legal, clients, employees, media)?

Y N

Have you adopted the framework?

Y N

Can you quickly detect an attack in progress or identify a breach in progress before significant damage occurs?

Y N

Does your organization understand that a significant threat arises from internal resources?

Y N

Do you have the entities identified who will quickly help you to 'fill the gaps'?

Y N

Are you protected against vulnerabilities to your applications?

Y N

If you have answered 'no' to any of these questions, you may be exposing your organization to threats. With limited budgets and resources, it continues to be a challenge for most to manage their cybersecurity posture and to remain compliant. The demand for information security leadership and implementation guidance has never been higher. However, with demand comes supply and this has created a shortage of such resources resulting in two main problems: scarcity of skilled security resources and their increasing costs.

If you have answered 'no' to any of these questions, you may be exposing your organization to threats. With limited budgets and resources, it continues to be a challenge for most to manage their cybersecurity posture and to remain compliant. The demand for information security leadership and implementation guidance has never been higher. However, with demand comes supply and this has created a shortage of such resources resulting in two main problems: scarcity of skilled security resources and their increasing costs.

CYBERSECURITY WORKFORCE SHORTAGE
to reach **1.5** million by **2019**

In January 2016, Forbes reported there were 1 million cybersecurity job openings in 2016 while Cybersecurity Ventures conveyed in their Q4 2016 report, Cybersecurity workforce shortage to reach 1.5 million by 2019. This spwned the real question asked by the Fast Company in 2016, "Can armies of interns close the cybersecurity skills gap?" Inevitably doubtful. Forbes dissected this notion and found that United States graduates are majoring in computer science programs that contain little to no cybersecurity courses. In addition, companies are looking to meet the demand by cross training their current security staff. Together, this makes a dangerous mix of green, unqualified resources managing your cybersecurity framework.

This is where a Virtual Chief Information Security Officer (vCISO) service can prevent a costly liability and safeguard your assets. By partnering with Enterprise Integration (EI), an onshore IT MSP powered by digital robotics, you will gain over 20+ years of IT and Information Security experience in supporting Fortune 500 clients. EI has developed tailored vCISO policies, procedures, automated processes and innovative toolsets that can be leveraged for your business at a fraction of the cost of what it would take to build and implement them in-house.

WHY IS THIS IMPORTANT?

Technology trends are intersecting with business trends and cybersecurity has become the costly, central focus. According to the 2017 PWC Global State of Information Security® Survey 2017, "55% of survey respondents say they collaborate and share information with others to improve cybersecurity."

Partnering with EI, presents an opportunity to join forces and better understand the cybersecurity landscape, quickly adjust security controls to address evolving threats and help you make more informed investments to address the most significant cybersecurity risks.

EI's vCISO service is a fractional model that is changing the economic model of your information security spend. Both from an innovation and from a risk mitigation perspective, EI's vCISO value consists of:

- A fractional cost model
- CISO-level security knowledge and expertise
- Access to pre-defined and easy to implement Security Frameworks, Policies and Procedures
- Access to tried and tested Enterprise-level Tools, Processes and Best Practices
- Guidance to your team(s), and participation in Leadership and Security/IT steering committee(s)
- Compliance & Audit oversight
- Thought Leadership

HOW DO WE DO IT?

At a flat monthly rate, each vCISO will deliver information security services backed by EI's experienced information security consultants and a team of security analysts and advisors. From a menu of options, you get to decide which vCISO services you want. EI offers vCISO services in 3 main categories: Technology Solutions, Risk and Compliance Management and EI LABS.

1. Technology Solutions

New security products are introduced as quickly as the threats and business issues they are intended to address. EI's Security Technology Solutions ensure that companies make sound infrastructure investments by evaluating best practice options. Once a solution has been chosen, our engineers ensure it is successfully implemented, configured and managed.

- Firewall / UTM Management
- Security Event Correlation and Log Management
- Vulnerability Assessments
- Virus, Spam and Spyware Protection
- Advance Persistent Threat Protection
- Content based redirection and blocking
- Load Balancing
- Application Firewall
- Single Sign-on
- Automated User Provisioning and De-provisioning

- Data Loss Prevention
- Mobility and Wireless
- VPN

2. Risk and Compliance Management

Bridging the gap between risk, compliance, corporate governance, and information technology is a major objective in today's business climate. EI's Risk and Compliance Management practice helps clients build and manage ongoing programs to manage risk and meet regulatory standards while optimizing business operations.

- Security Program Review
- Security Policy Review and Development
- Security Roadmap Development
- Security Controls Development
- Security Risk Assessment
- Compliance Gap Assessment
- Vendor Risk Assessment

3. Enterprise Integration Labs

Without an accurate measurement of an organization's security posture, it is impossible to know its strengths and weaknesses. EI LABS, the security assessment and vulnerability research group, helps clients determine the gaps between current and desired security postures and develop a roadmap for remediation.

- Enterprise Penetration Testing
- External and Internal Security Assessment
- Application Security Assessment
- Wireless Security Assessment
- Mobile Application Vulnerability Assessment
- Social Engineering
- Security Training
- Vulnerability Research

AUTOMATION AND DIGITAL ROBOTICS TOOLSUITES

EI is changing the economic model of IT operations by making IT the most efficient onshore capability and at a better price point than was previously experienced over the last 20 years. This paradigm shift is being powered by automation and digital robotics to autonomously identify placeless work or menial tasks, enabling EI's resources to stay ahead of opposing threats.

EI's team of information security consultants, advisors and analysts have access to a multitude of innovative and automated tool suites. Your vCISO inherits these enhanced capabilities to continually help your business discover how to manage its Security infrastructure. Coupling automated tool suites and EI's strict adherence to an industry-leading information security service framework, your vCISO will create a full

costly, "hidden" cyber services. This proves your vCISO functions as an extension of your business, while delivering expert security insight, leadership, and support.

SERVICE DELIVERY INTELLIGENCE™ (SDI™)

Providing an Enterprise view of your entire Security Posture by connecting and correlating all of your data into a single, humanized interface that creates client-centricity.

SDI™ ENDPOINT EXPERIENCE

Continuously and comprehensively monitors your end point performance and health of your organization.

DIGITAL ROBOTICS ENGINE™ (DRE™)

Programmatically fed by the SDI™ tool suite, this expert system correlates the health and delivery of data to the business, without human intervention.

INDICATOR OF COMPROMISE™ (IOC™)

Dramatically reduces response time in identifying threats through EI's proactive detection tool.

CRYPTOWATCHER™

Proactively detects and eliminates ransomware attacks

EXPERTISE

- Certifications held by EI's vCISO consultants and analysts:
- Certified in Risk and Information Systems Control (CRISC)
- IT Infrastructure Library® (ITIL®)
- Certified Ethical Hacker (C|EH)

CONCLUSION

EI provides professional information security services every day, it is not just a concept. Security is at the core of EI's service portfolio and has been for over 20 years. EI's vCISO offering has been developed to address your businesses cyber security needs. At a fraction of the cost, it will maximize the quality of your IT and Security deliverables across your entire organization. By partnering with EI, your company will fortify its security posture and shape a culture of security-conscious employees and executives.

> "EI'S VIRTUAL CISO TEAM TRULY UNDERSTANDS OUR INFORMATION SECURITY NEEDS, OUR ENVIRONMENT, AND OUR BUSINESS. EI PROVIDES US WITH INNOVATIVE TECHNOLOGY SOLUTIONS, EXPERT SECURITY INSIGHT, LEADERSHIP, AND SUPPORT, TO KEEP OUR MOST IMPORTANT ASSET, OUR DATA, SAFE."
>
> *– TIM WERNER, PRESIDENT OF BLUESTAR RETIREMENT SERVICES*

ENTERPRISE
INTEGRATION

REDUCE IT INDUSTRY SPEND

entint.com | 888-848-9332 | info@entint.com

RESOURCES

1. Steve Morgan. United States. Forbes. One Million Cybersecurity Job Openings In 2016

2. Cybervista. United States. Cybersecurity Ventures. Cybersecurity workforce shortage to reach 1.5 million by 2019

3. Monty Munford. United States. Fast Company. Can Armies of Interns Close the Cybersecurity gap?

4. Steve Morgan. United States. Forbes. Top U.S. Computer Science Undergrad Programs Flunk Cybersecurity

5. United States. PWC. Global State of Information Security® Survey 2017