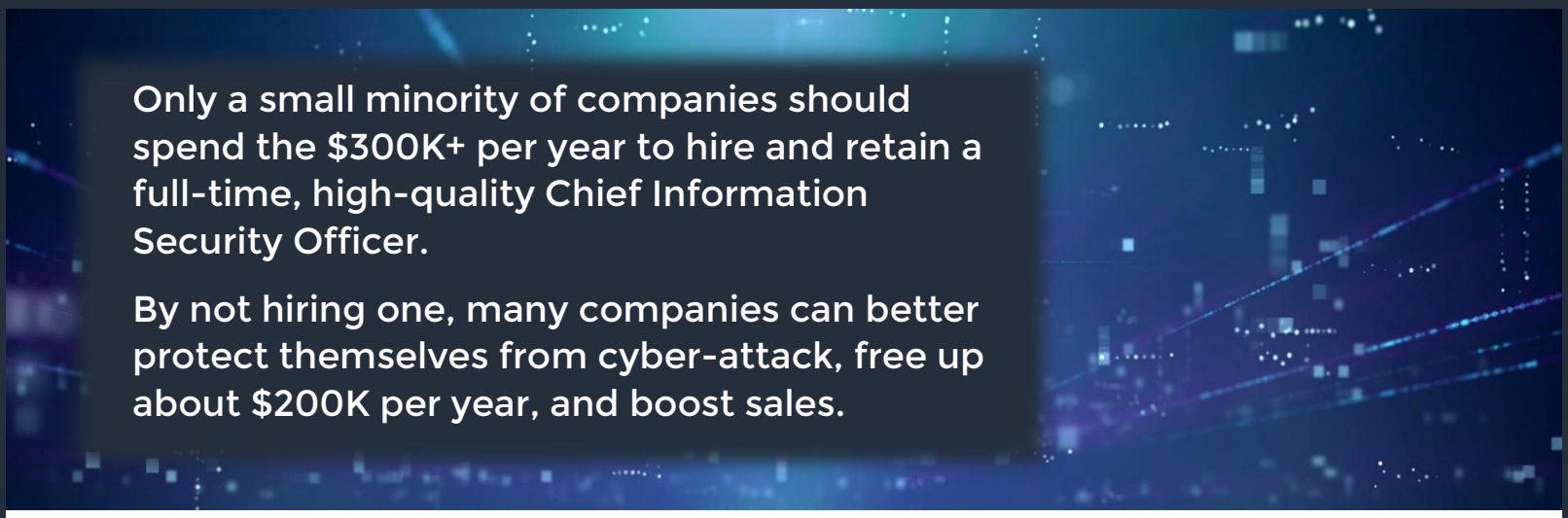
HIRING A FULL-TIME CHIEF INFORMATION SECURITY OFFICER CAN BE AN EXPENSIVE MISTAKE



Elliot Turrini, Practical Cyber CEO, & Dr. Marc Rogers

The bottom line: By not hiring a full-time Chief Information Security Officer ("CISO"), many companies can better protect themselves from cyber-attack, free up about $200K per year, and boost sales.

Skeptical? Consider that many of the worst cyber-attacks over the last 5 years have occurred on the watch of a full-time CISO; and that these cyber-attack victims were following the traditional cybersecurity approach that has repeatedly failed and is even more dangerous considering today's already substantial and rapidly growing cyber risks.

"Insanity is doing the same thing over and over and expecting different results."

Who should hire a full-time CISO? A small minority of today's total number of organizations should hire a full-time CISO – particularly profitable organizations with 5,000+ employees in security-sensitive and highly regulated industries such as financial, government, healthcare, and pharma. The larger the organization, the more profitable, the more highly regulated, and the more it will lose from cyber-attacks; the greater the justification to pay $300K+ per year to retain an effective CISO. That leaves a large majority of organizations that should consider foregoing a full-time, traditional CISO.

The 3 main reasons not to hire a full-time CISO: A large majority of organizations should not hire a full-time CISO for the following reasons:

1. **EXPENSIVE & HARD TO RETAIN:** Well-qualified, full-time CISOs are hard to find, expensive, and difficult to retain. With benefits, they typically cost close to $300K per year and change jobs often because of high demand.

2. **NOT SUFFICIENTLY EFFECTIVE:** Even many well-qualified CISOs are not as effective as some less expensive alternatives:
    - Many CISOs perform mostly high-level functions (e.g., setting strategy) that you need in small doses (e.g., about 4 weeks per year) and can get elsewhere for less.
    - Too many CISOs are missing important aspects of the multidisciplinary expertise required to protect your organization from the financial harm of cyber-attack (e.g., cyber risk transfer via contract and insurance).
    - Too many CISOs fail to implement enduring processes that make your company more self-reliant, resilient, and less vulnerable to cyber-attack.
3. **DON'T BOOST SALES:** Too many CISOs lack the skills to assess your market and produce the security/privacy marketing and sales materials that will help you boost sales.

What you must know to make the right "CISO" decision: To make the right "CISO" decision, you must know the following:

1. How your organization should actually address cyber-attacks. Hint: it is far more than just the traditional cybersecurity approach; and it avoids dangerous deference to cybersecurity technologists. Use a profit-centric approach.
2. The truth (and limitations) about how full-time CISOs typically help organizations, and the challenges of finding and retaining high-quality CISOs. Hint: Make a detailed list of what you think your full-time CISO will do; it won't justify $300K+ per year.
3. How to objectively compare a full-time CISO with alternatives such as an external multidisciplinary team (like Practical Cyber) or a virtual CISO. Ask us. We can help.

To learn more, including receiving our article detailing the information about making the right "CISO" decision, email Elliot Turrini at Elliot@PracticalCyber.com.

ABOUT THE AUTHORS

Elliot Turrini, JD: He is the CEO of Practical Cyber, a multi-tool, multidisciplinary cyber and privacy risk mitigation consulting firm. He has been a federal cybercrime prosecutor, a cyber/privacy lawyer, and a serial entrepreneur. He is the co-editor of the book Cybercrimes: A Multidisciplinary Analysis, and is now a cyber and privacy risk mitigation expert.

Dr. Marc Rogers: He is an internationally renowned cybersecurity expert, founder of MKR Forensics, former law enforcement official, has 25+ years practical cybersecurity experience, and is a tenured cybersecurity professor at a major university.