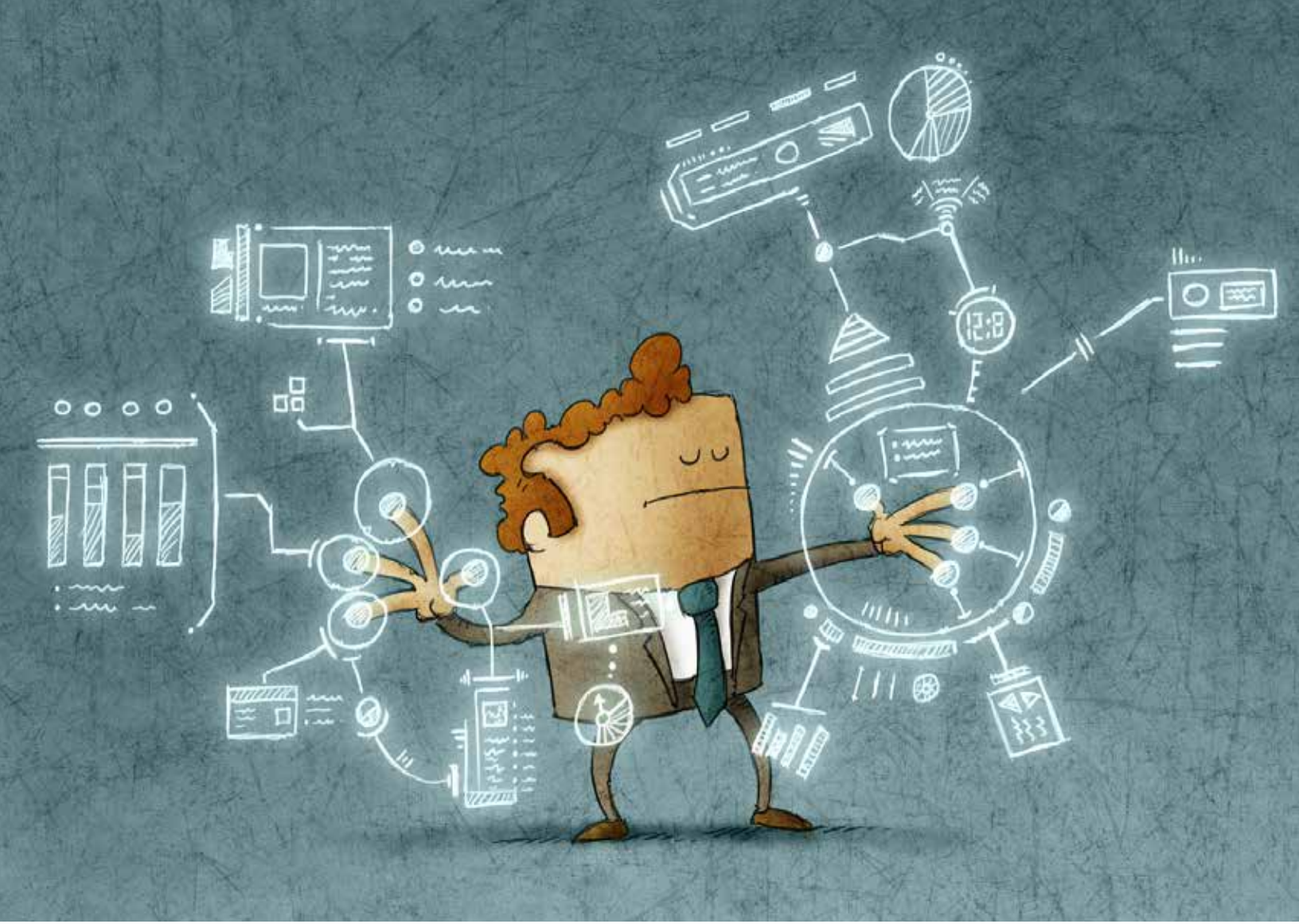


The Making of the Modern CISO

Evolving Risks, Roles, and Rewards

SAI GLOBAL

CISOs in the making

Information Security (InfoSec) professionals who thrive to fight cyberattacks may be on a career path to rise to the level of Chief Information Security Officer (CISO). Even now, a fairly significant number shoulder many of the same risks and responsibilities that are inherent to the CISO position.

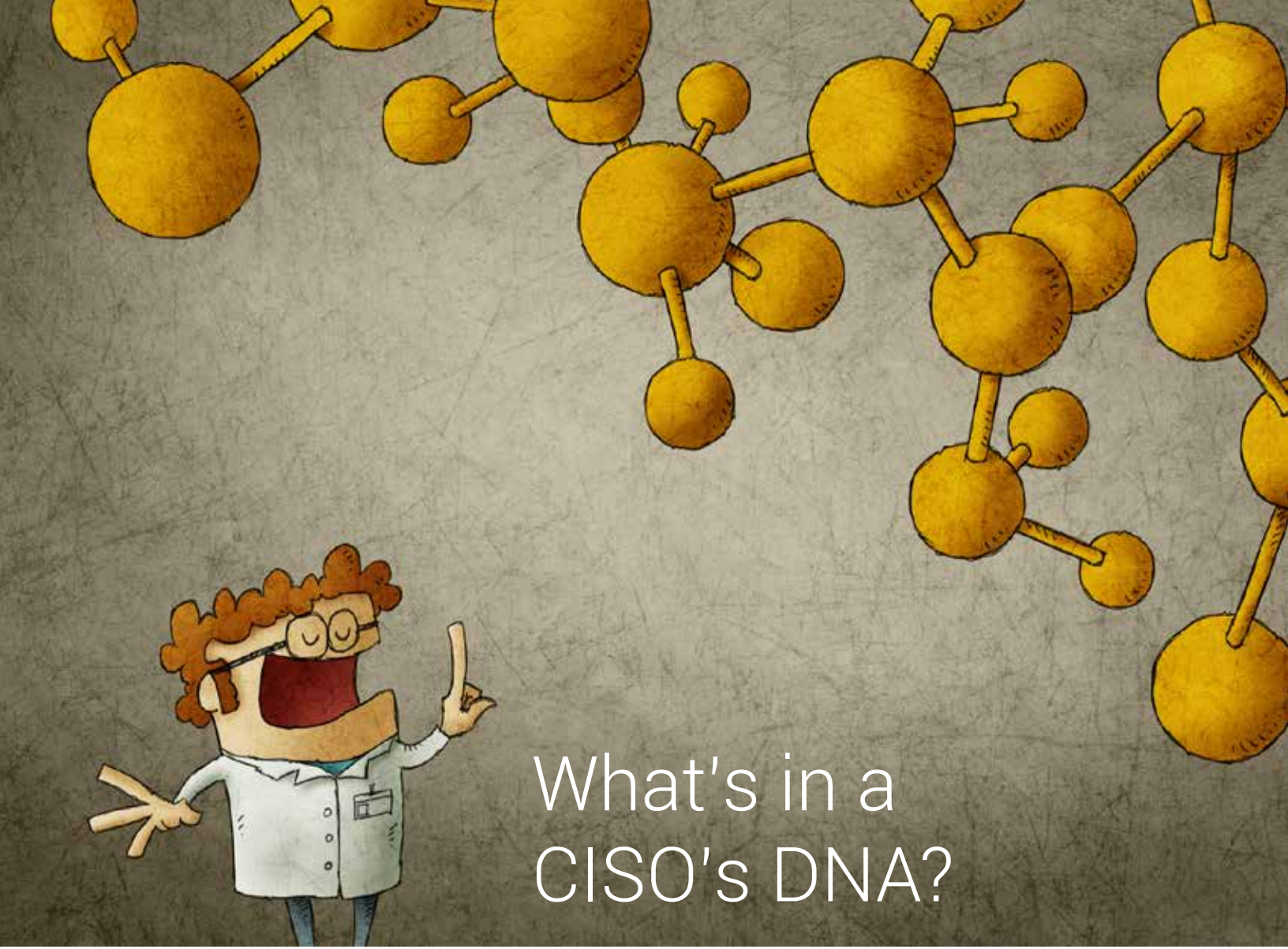
And the industry needs more prospective candidates who set high personal goals and grow from their experiences. Fortunately, future CISOs are already amassing experiences that inform their work.
Get to know the modern CISO and their making. A collection of insights from top CISOs and business experts awaits.

Demonstrating traits that map to CISO success

The origins of the modern CISO

Given all that CISOs have become, it's hard to imagine that the position did not exist less than a generation ago. But, if it wasn't for one high-profile attack, the CISO might never have been. In 1995, Russian hacker Vladimir Levin launched the first electronic bank heist that used a PC.[1] The incident made global headlines.

Citibank recovered all but $400,000 of the missing $10 million. What the attack foretold for the future of information security prompted Citicorp, the bank's parent company, to christen the world's first CISO, Steve Katz,[2] in preparation. Since then, evolving attacks and threats have become commonplace. The modern CISO is adapting for what lies ahead.



What's in a CISO's DNA?

Not everyone has what it takes to be a CISO. Favorable personal characteristics and instructive career paths are evident among suitable professionals.

Some experts say the InfoSec professional's career roadmap is pivotal to their advancement. "An aspiring CISO should come out of an enterprise operations role, preferably one that includes both stints as a technical expert or contributor as well as a variety of progressively responsible management positions (manager, director, VP, and so forth)," says Ed Tittel,[3] a veteran of the IT/IS industry. There are benefits to coming up through the ranks and doing the work you'll eventually lead others in doing.

FACT

The CISO role is evolving rapidly, so there is no standard guidebook to getting hired, progressing, or succeeding as a CISO.[4]

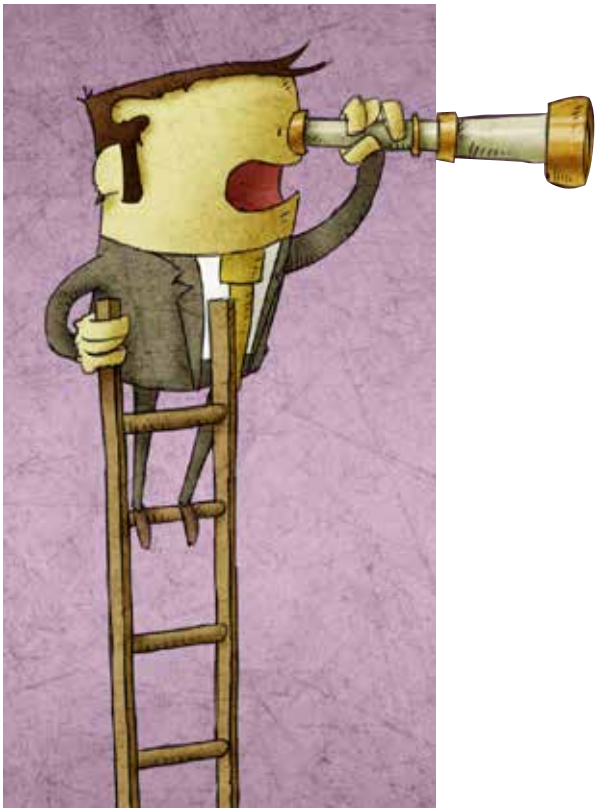
- Forrester Research report: CISO Career Paths: Plot Your Course For Advancement, December 2017

Essential CISO habits

Courtesy of Hersh Shefrin, Mario L. Belotti Professor of Finance, Leavey School of Business, Santa Clara University:

- *Serve* others
- *Seek* challenges
- *Set* high personal goals
- *Search* for clues to the InfoSec puzzle

Others confirm the security professional's character as superior when it comes to reaching this office. "For example, people who have high personal goals, a desire to serve others, and a need to seek success have a head start on making the grade," according to Shefrin.[5]



Top CISO traits

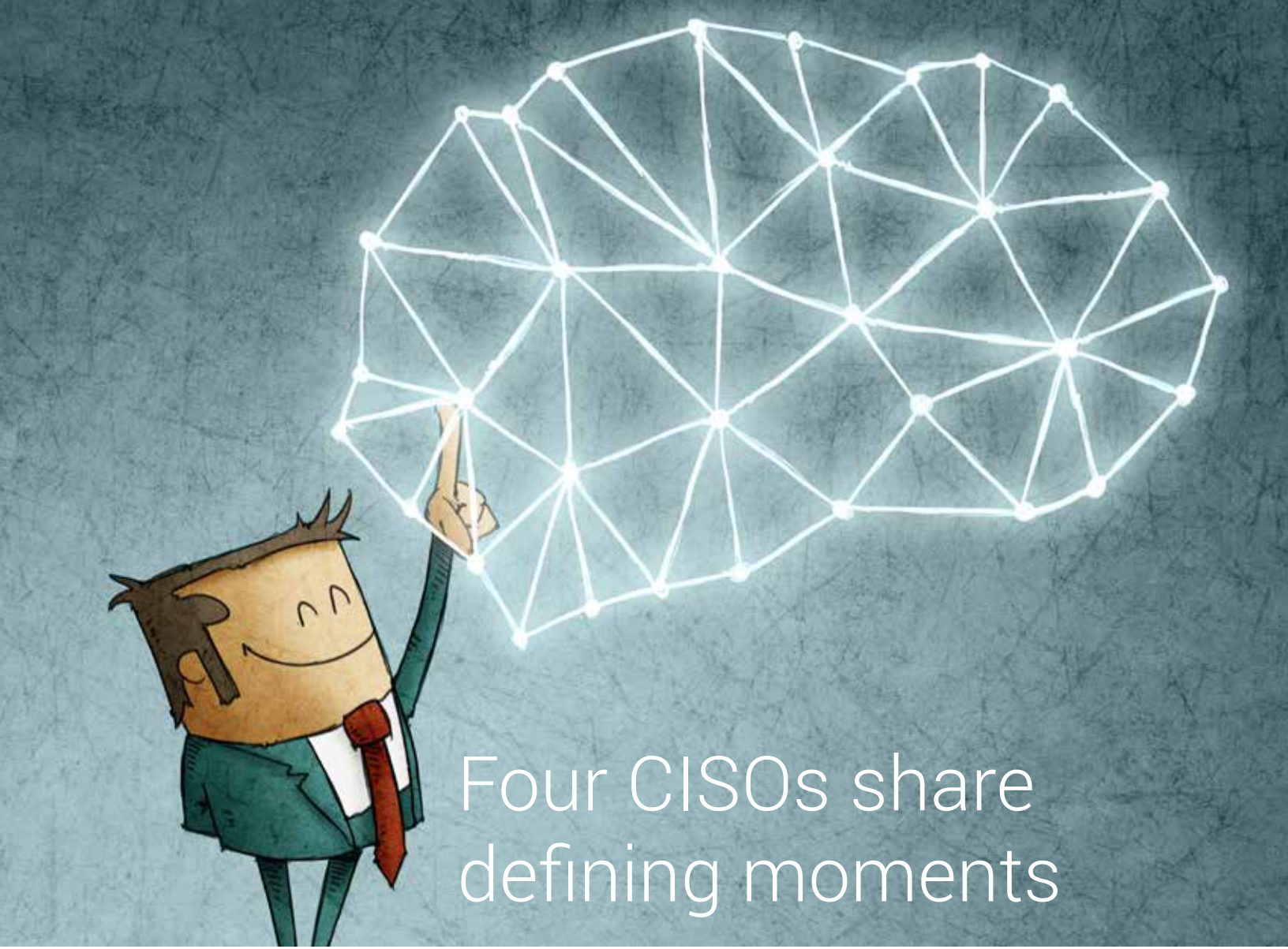
- Conscientious
- Agreeable
- Empathic

"Eventual CISOs are agreeable, play well with others, and interact empathically. They possess a strong theory of mind: they engage with you in a way that, if something is happening in your life, they feel it the way you feel it," says Shefrin.

"CISOs need to feel like guardians. They're not simply solving a problem: there's a broader meaning to the problem, as well," adds Shefrin.

Candidates who crave challenges and excitement find the battle against cybersecurity risks attractive. Budding CISOs enjoy hunting for clues, following where they lead, and finding answers that solve complex, puzzling issues.

"Good habits and traits weigh heaviest in making the modern CISO, though you should not leave a unique, personal, and illuminating career path undone," explains Shefrin.



Four CISOs share defining moments

Defining moments shape priorities for people who later occupy the CISO position. Rare anecdotes from leading CISOs provide transparency into such serendipitous experiences.

One CISO's transition from pen tester

Working in the trenches can force you to examine security vulnerabilities up close. Stints in finding system flaws then managing risk from a higher vantage point can reinforce critical skills. Such was the case with Frank Aiello,[6] CISO, the American Red Cross.

Early in his career, Aiello worked as a penetration tester at a security consulting firm before becoming the company's security practice lead. These positions enabled Aiello to see risk from different angles, which contributed to the CISO that he would become.

"It helped me expand my *thinking*. Instead of seeing security in black and white terms, I saw the risk, and risk management. I learned to translate security into business terms," says Aiello. "This was the key shaping experience for me."

Realizing the rewards of protecting his family and the enterprise

Realizing your exposure as your identity lies bare on the web can be a jolt of reality. That wake-up call could be the beginning of a life of defending identities, data, and privacy. This was the outcome for Gerald Beuchelt,[7] CISO, LogMeIn.

Beuchelt began to understand the rewards of protecting Personally Identifiable Information (PII), data that identifies an individual—after he Googled his last name. Because he found so much specific, private information online so easily, he began to engage more deeply in identity security.

"It motivated me to start thinking about how to protect my life, my security, and the security and privacy of my family. I apply what I learned to larger organizations to help other people as well," Beuchelt explains. "The work is very fulfilling."

Security breaches inspired a blossoming CISO

Facing the barrage of breaches that entangle the enterprise can sharpen your senses and build a relentless determination to extricate the business from cyberattacks. Jackson Muhirwe,[8] Deputy CISO, the University of California, Davis, found himself in this situation in a previous role.

As a cybersecurity program manager, Muhirwe came face to face with the onslaught of cyber threats. It forged his thinking about the security organization. "The breaches were the big difference for me. They inspired me to do better, so I could provide solutions," says Muhirwe.

Forces shaping modern CISOs

War games help CISOs train their brains.

CISOs shoulder increasing responsibility for enterprise risks and cyberattacks. The burden comes with a psychological cost. Responsibility exposes CISOs to emotions of regret and pride.

These emotions amplify the impact of good and poor decisions and outcomes in the CISO's mind. Knowing their strengths and weaknesses relative to people they engage will help CISOs cope with shifts in passion and sentiment. CISOs can use war games to test their mettle in this regard. War games help CISOs train their brains. Simulating specific types of cyberattacks can improve IT security's incident response as well, according to CSO magazine.[9]

Coping with breach-related loss

Nothing brings the realities of breaches home like a personal loss. In the case of Richard Rushing, CISO, Motorola Mobility, a soon-to-be-infamous piece of ransomware infected a company laptop in the care of one of his employees. The attack encrypted the employee's device, along with five years of personal photos, baby pictures and videos which, unfortunately, hadn't been backed up.

The employee asked the CISO if the photos and videos could be saved. *"At that moment, you see that person sitting across from you and you must have that conversation with them. It touches you. It stays with you for a long time,"* says Rushing.

Changes for the modern CISO

The job of CISO has undergone radical changes over the past few decades. The CISO's biggest roadblock was often convincing the board to spend on cybersecurity. Now, it's finding solutions to the many security threats. It's almost like being a firefighter when alarms are constantly going off.

Today's environment of constantly evolving cyberattacks means that those alarms are louder and far more routine. Modern CISOs must be able to adapt to a full-blown hacking industry that profits from stolen funds, customer data, and intellectual property. The global cost of "cybercrime damage" was more than $3 trillion in 2015. That figure will balloon to $6 trillion annually by 2021,[10] according to the *2017 Cybersecurity Ventures Official Annual Cybercrime Report.*

"It's not the cost. Instead, you get bogged down in depreciation, capitalization, the OpEx, and CapEx stuff that used to be very simple," says Rushing.

The CISO is steering a broader security organization to respond to the onslaught of attacks. The InfoSec group is involved with various functions: CISOs are dealing with e-discovery, regulatory and compliance issues, legal issues, and physical security.

You can add financial responsibilities to the burgeoning list of business hats that the CISO must wear. “We're getting stuck in budgetary cycles,” explains Rushing.

Modern CISOs are like pilots, steering cybersecurity's soaring evolution and impact on the business.

By taking some exemplary CISO habits and traits as starting points, the industry can form additional role requirements that anyone aspiring to the position should be able to meet.

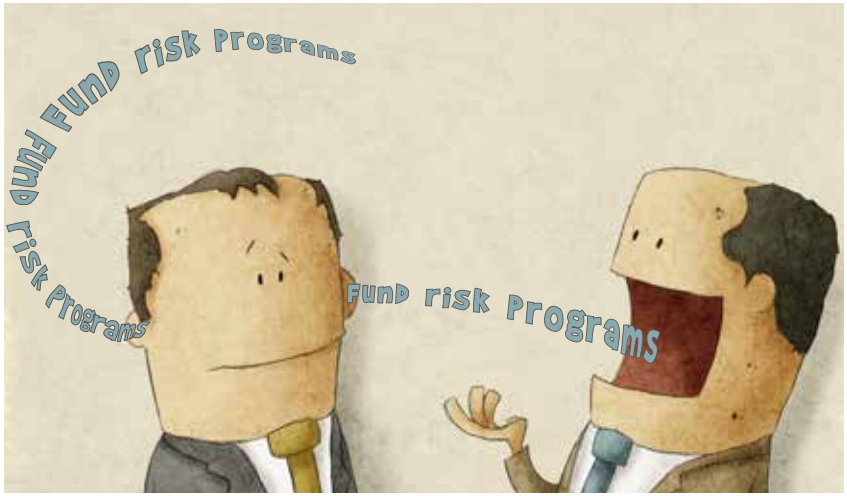
Three bold requirements for strategic CISOs

- Strategic CISOs keep self-doubt from breaching their psyches. "When you're **confident**, you're comfortable in your own skin. You welcome accountability and are not afraid of the risk and responsibility that comes with being a **bold decision-maker**," says Sarah Hathorn,[11] CEO, Hathorn Consulting Group, a corporate DNA consultancy.

- CISOs must **showcase strong security postures** for **prospective customers** to **earn** their **trust**, per BitSight.[12]

- "CISOs need to strike a **balance between security requirements** and **business conditions** to allow the **company** to **expand quickly** and **innovate swiftly** while **maintaining data confidentiality and integrity,**" says Gerald Beuchelt, CISO, LogMeIn.

Technical terminology is often foreign to many C-levels, the board and much of the business. Translating IT-specific language for the business means more than just communicating the same message using a different vocabulary.



How CISOs translate technical jargon

"In many ways, the new CISO is the bridge in communication between the technology and business executives, who often speak different languages. Having a CISO with the technical background who is able to translate technology into risk allows for the CRO to have a more effective impact on the perceptions of the board," according to Kacy Zurkus, in "CISOs bridge communication gap between technology and rise," in the December 13, 2016, issue of CSO magazine.[13]

How CISOs talk with the board

"We're going to continue to see the CISO role, the security industry, and the security function move even closer to the board," says Frank Aiello, CISO, the American Red Cross

One way of measuring a CISO's performance is by how adept they are at filtering their messages for the boardroom.

When you present to the board

1. “Avoid heavy technical metrics and point to the big picture and what it means to the business,” says Beuchelt. “Help them understand the risk profiles of various functions and the options to treat that risk.”

2. “Include data about what the competition is doing and how the company measures up to them. Discuss your comparable maturity in the marketplace,” says Rushing. Competitor analysis supports the board’s planning initiatives.

This movement will drive CISOs to prioritize and deliver critical data in terms the board can appreciate.

Fast forward to the future of the CISO

91% of cybersecurity pros fear hackers will use AI to attack their company, according to Webroot.

The CISO's challenges are forever fluid, living, and dynamic. The big issue of tomorrow is weaponized AI.

"The malicious use of AI concerns me," says Beuchelt, who confirms that hackers will use AI to:

- ***Impersonate*** people's voices
- ***Edit live video*** without detection
- ***Orchestrate attacks across many attack vectors at once***, including mass-targeted spear phishing

"We will talk about malicious AI for years to come," adds Beuchelt.

Still, there is great hope for the future of cybersecurity. The security industry is responding to its challenges. Rushing says, "With the constant flood of breaches, security is improving and employees are becoming more aware, understanding security, and playing their role."

About the participants

Gerald Beuchelt

Chief Information Security Officer
LogMeIn

Gerald Beuchelt is the chief information security officer for LogMeIn. He is responsible for LogMeIn's enterprise security, compliance, and technical privacy program.

In his previous role, Beuchelt was the chief security officer for Demandware, a Salesforce company, responsible for the information security of its Commerce Cloud. He was also the acting chief privacy officer and data protection officer for Demandware's German subsidiary.

At MITRE, Beuchelt was a principal information security engineer, focused on securing web services, information assurance, and identity management technology and applying these technologies in the context of complex government environments. In this role, he worked closely with technical standards communities, business partners, and suppliers, as well as senior representatives of MITRE's government sponsors.

Previously, he worked for Sun Microsystems, Inc., in various roles, including the Business Alliances Group of Sun's Chief Technologist's Office.

Beuchelt holds a Master of Science degree in theoretical physics.

About the participants

Frank Aiello

Executive Director and Chief Information Security Officer
American Red Cross

Frank Aiello is the executive director and chief information security officer of the American Red Cross, responsible for overseeing and coordinating the IT security program across the enterprise. He is an experienced IT leader with more than 19 years of business and technical experience, specializing in information security, risk management, and regulatory compliance.

Prior to joining the Red Cross in 2009, Aiello was a vice president managing the Washington, DC, office for a midsize consulting firm. Prior to that, he was a mid-Atlantic technology practice leader for a Big Four accounting firm, where he served large corporations across a variety of industries, including financial services, telecommunications, and energy, as well as federal agencies. Frank is a frequent speaker on information technology and risk management.

Aiello has a Master of Science degree in software systems engineering from George Mason University and a Bachelor of Science in computer science from Penn State University.

Richard Rushing

Chief Information Security Officer
Motorola Mobility LLC

Richard Rushing is the chief information security officer for Motorola Mobility LLC. He leads the company's security efforts, having developed an international team to tackle the emerging threats from mobile devices, plus targeted attacks and cybercrime.

Prior to joining Motorola Mobility, Rushing was co-founder and chief security officer of AirDefense, a manufacturer of wireless security systems that was acquired by Motorola in 2008. Over the course of his experience in networks and security systems at Siemens, GE, SecureIT, and Verisign, Rushing organized, developed, and deployed practices, tools, and techniques to protect the intellectual property of these worldwide enterprises.

He participates in several corporate, community, private, and government security councils and working groups, setting standards, policies, and solutions to current and emerging security issues. A much-in-demand international speaker on information security, Richard has presented at many leading security conferences and seminars around the world.

About the participants

Jackson Muhirwe, PHD, CISSP, C|CISO

Deputy Chief Information Security Officer
University of California, Davis

Jackson Muhirwe currently serves as the deputy chief information security officer at the University of California, Davis. Key among his responsibilities is leading the information security risk management program.

Prior to joining UC Davis, Muhirwe worked for the City and County of San Francisco as the director of cybersecurity services in the Department of Technology and as interim city chief information security officer (CISO). As the citywide CISO, he was charged with understanding the business needs of the city and establishing an information security management program ensuring that its information assets were adequately protected.

Before joining the City of San Francisco, Muhirwe worked in academia as a professor directing cybersecurity programs.

Muhirwe holds a PhD in computer science, CISSP and C|CISO.

References

[1] www.nytimes.com/1995/08/19/business/citibank-fraud-case-raises-computer-security-questions.html

[2] chapters.theiia.org/Orange%20County/IIA%20OC%20Presentation%20Downloads/2014%20Joint%20IIA%20ISACA%20Spring%20Conference/Tom%20Borton%20-%20Evolution%20of%20the%20CISO.pdf

[3] www.businessnewsdaily.com/10814-become-a-chief-information-security-officer.html

[4] www.forrester.com/report/CISO+Career+Paths+Plot+Your+Course+For+Advancement/-/E-RES141371

[5] www.linkedin.com/in/hersh-shefrin-574a4522/

[6] www.linkedin.com/in/aiellofrank/

[7] www.linkedin.com/in/beuchelt/

[8] www.linkedin.com/in/muhirwe/

[9] www.csoonline.com/article/3203706/security/using-cyber-war-games-to-improve-incident-response.html

[10] cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[11] hathornconsultinggroup.com/blog/exude-confident-executive-presence/

[12] www.bitsighttech.com/blog/chief-information-security-officer-roles-responsibilities

[13] www.csoonline.com/article/3149149/security/cisos-bridge-communication-gap-between-technology-and-risk.html

About SAI Global

SAI Global, a provider of integrated risk management solutions, assurance and property services, helps organizations proactively manage risk to create trust and achieve business confidence, growth, and sustainability.

Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. We are a trusted provider of standards, technical information and regulatory content to organizations globally. Our accredited audit and certification services, based on third-party endorsed management systems and world-class training, help organizations gain efficiencies, improve performance and ensure compliance. In Australia, we are largest provider of property information and settlement services and support confident decision making across all stages of the property lifecycle.

Underpinning all of our solutions are proven and trusted business methodologies, powered by local expertise and know how. The company has global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

For more, visit www.saiglobal.com.

SAI GLOBAL