PECB

When Recognition Matters

WHY EVERY COMPANY NEEDS A CISO?

We are living in an environment where dramatic news, reports, events and incidents about information security have become our daily news and very familiar pattern. All these failures have caused that information or better to say information security to become a top concern for every organization, company and even state.

Great improvements in technology, plans, policies, objectives, self-hacking-audits, trainings, awareness activities, entire management systems, information security teams inside of organizations and business now are giving enormous attention to mitigate the information security risks.

As always, there will always be companies which will add more components to this and will invest even more in information security, and also those which will consider that there is no need for all these things. One of the main topics regarding this issue is: Should or should not every company have a Chief Information Security Officer (CISO) role?

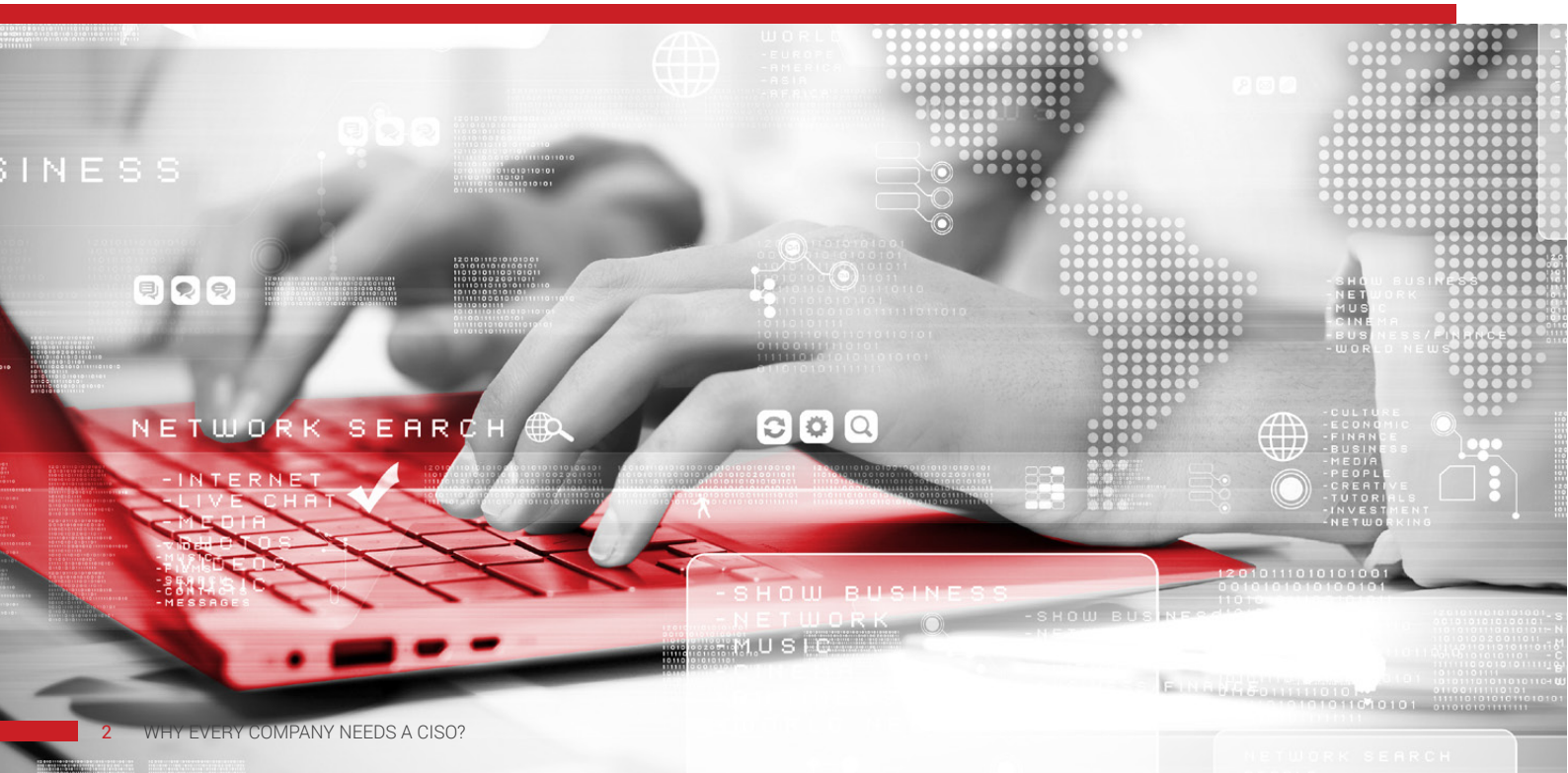
In different sources you can find that CISO should be responsible for information security and information assurance, regulatory compliance, risk management, supply chain risk management, cybersecurity, and information technology controls, privacy, computer emergency response team, access management, security architecture, IT Investigations, digital forensics, and eDiscovery, disaster recovery and business continuity, security operation centers, etc. So who would oppose to a CISO role? Is CISO needed within a company? The answer is: Yes indeed.

However, will it ever be possible to find a person who would be able to maintain all these components? The answer is: Never, but it is CISO's obligation to lead a security professional team which will take care of all these components.

"The security guy really needs to understand the business risk, because a CISO's job is not to protect IT, it's to protect the business from the IT infrastructure." *Rick Doten, CISO, Digital Management Inc*

CISO should be a connecting bridge between executives and engineers. He/She should navigate the details of technology controls and compliance frameworks, moreover, should go further and deeper than just to make operational security but develop and direct long term security plans.

A CISO should be able to understand the interaction between business processes and information security together with technology used in organization, so he/she would be able to give his/her opinion and even take decisions about company's security activities if they are well-aligned with the projects that the business is undertaking.



So it is CISO's role and his/her team to direct technical staff and to ensure business objectives and risk tolerances. He/She should be a good communicator with senior members, board of directors and other involved parties, and try to explain in most simple and understandable way technical issues connected with business risks and objectives.

A CISO role should be involved also when the company decides to implement new technology, something innovative or modernize the existing ones. Security teams leaded by the CISO have to take care of implementation and validation of chosen technology which should be appropriate with company security policy, but also enable the business.

He/She should be able to act immediately when somethings goes wrong within company or the company has been breached, what to do, whom to communicate, how to locate and to stop the result of the breach quickly and efficiently, and what to do to prevent this from happening again.

Furthermore, he/she should have knowledge on legal and compliance issues. Moreover a person who will have knowledge about technicality about information security and management most probably would be able to do public speaking within the company, conferences, and seminars. To have an information security expert to present successful stories, ideas and regulation systems or even information security topics which would result in best marketing possible for the company.

So, there are a lot of reasons why a company should consider the CISO's role, however, as in every issue there are also a lot of pros and cons toward this issue as well. The cons toward this issue are connected with the fact that most companies already have a Chief Information Officers CIO, Chief Risk Officers CRO and Chief Privacy Officer CPO, so adding one more will create just more official procedures, conflicts and confusion within the company. The response to this is found very easy. CIO Chief Information Officer is a title given by the company to enhance the importance of information at C level, which is very reasonable and smart decision. Information is everything and everywhere, however, threats and vulnerabilities toward it have never been higher than nowadays, so, it is more preferable to split up the role of CISO with others so that every Information Security program can have at least a leader who will be responsible to "secure" Information Security.

"I'm amazed to hear that large organizations still don't have a CISO. When it comes down to it, I don't really know too many businesses that can operate without [IT], and security is just a fundamental component of everything that companies have to do now." *Chris Ray, CISO, Epsilon*

There are already some international standards like ISO 27001 that have added the role of CISO in every documented information security policy with a senior position created to oversee and manage that policy, so what is left is just to look for a professional certified expert who will take care of the company.

PECB International is a certification body for persons on a wide range of professional standards. It offers ISO 27001, ISO 27002, ISO 27005, ISO 20000 and ISO 22301 training and certification services for professionals wanting to support organizations on the implementation of these management systems.

ISO Standards and Professional Trainings offered by PECB:

- Certified Lead Implementer (5 days)
- Certified Lead Auditor (5 days)
- Certified Foundation (2 days)
- ISO Introduction (1 day)

Lead Auditor, Lead Implementer and Master are certification schemes accredited by ANSI ISO/IEC 17024.

Rreze Halili is the Security, Continuity and Recovery (SCR) Product Manager at PECB. She is in charge of developing and maintaining training courses related to SCR. If you have any questions, please do not hesitate to contact: scr@pecb.com.

For further information, please visit www.pecb.org/en/training.