Security Scouts – Ensuring Integral Corporate Security for Tomorrow's Businesses

Written by Joshua Bucheli, Researcher und Editor in cooperation with Chris Eckert, CEO of Swiss Business Protection AG, and Peter Kosel, Founder of cyberunity

"know yourself and you will win all battles"
— **Sun Tzu**

In today's corporate world, where digital innovation and cyber-threats are advancing at breakneck speed, it is becoming all too easy to forget that 'Security' with a capital 'S' – or integral corporate security (ICS) – is a holistic discipline that extends beyond cyber-security.

Defending cloud systems and preparing encryption for the quantum age are indeed important elements of 21st century corporate security, but they do not replace the need for broader safety measures within a business.

Every business has assets that need protecting – **a proverbial 'golden goose'** – and all decisions ought to take the security of these assets into consideration. The problem is that, as it stands, vulnerabilities are often left exposed and missteps in security are redressed or even swept under the rug, rather than avoided.

This lack of awareness leaves businesses open to exploitation and makes it exceedingly difficult for them to detect and defend against threats – after all, how can you protect something if you don't know that it needs protecting?

As Chris Eckert, CEO of Swiss Business Protection AG, Program Director of the CAS in Business Protection at HWZ, and former Head of Investigations at the Zurich Cantonal Police points out, ICS is about supplementing reactive damage control with proactive reconnaissance, effective security measures, threat awareness, and training.

Where Does ICS Stand Today?

During his time as an external CISO and CSO, Chris observed first-hand how underdeveloped ICS strategies and corporate awareness put companies at risk:

He saw phishing emails impersonate a CEO and convince employees to transfer large amounts of company funds. He dealt with employees who had inserted unfamiliar USB drives into their work computers and compromised the business' cybersecurity. He even witnessed a case in which a flip-chart was left out after a strategic meeting and then photographed by an unauthorized individual after hours.

For now, it is safe to say that the security paradigm is reactive rather than proactive. Managers still pay limited attention to corporate assets and all too often, the issue of security is shifted onto IT departments rather than remaining the responsibility of managers.

Admittedly certain industries that face extensive external regulation and that are subject to regular audits like banking, pharma, and energy may be ahead of the curve in terms of integral security awareness.

The healthcare sector is also slowly but surely embracing the importance of ICS. In hospitals, where controlled substances and sensitive patient data are stored on premise, the necessity of managing access to restricted areas (both physical and virtual) and distinguishing between authorized personnel and any random John with a white lab coat is relatively well established. Nonetheless, there is still considerable room for improvement.

On the whole "ICS is still in its infancy – Everyone thinks they are insignificant enough not to be a worthwhile target and this is a mistake. From large international corporations to small local businesses, anyone can be a target. And yet, ICS only ever seems to make it onto companies' radars *after* they have become victims of fraud or espionage."

It is therefore imperative that businesses and managers embrace a more holistic way of thinking about corporate security instead of relying on IT specialists to perform damage control only after risky decisions and practices have led to unenviable consequences.

Here Chris stresses an interesting point about seeing security as an asset rather than a cost:

"At the moment, security is still seen as a business cost, with no prizes to be won. But hiring individuals who can ensure security in the workplace does not have to be a cost. In fact, with a little ingenuity it can be turned into a reputation that will entice partnerships and attract customers and clients."

Security Scouts – Hard Skills and Qualifications:

What businesses need above all else is for so called 'security scouts' to step up to the plate – individuals who can help them become aware of 1) their assets; 2) the threats that these face (both virtual and analog); and 3) how to go about integrating security measures that protect these assets into all levels of the business' activities.

These scouts will likely come from a variety of backgrounds, ranging from computer scientists, electronic technicians, business informatics specialists, and industrial engineers, to legal experts and professionals in commercial law, white-collar crime, finance, CSR, risk, governance, and compliance.

On this last point, a word of caution from Chris: “While beneficial, it’s important that individuals with these backgrounds avoid an overreliance on theoretical knowledge and emphasize their practical skills and experiences in their applications.”

The trick lies in combining these disciplines and the expertise that they bring into a comprehensive security team that will boost corporate security awareness. For example, criminologists and electronic technicians will be needed to sweep the business and its hardware for bugs, computer scientists and civil engineers will be needed to analyze blueprints for strategic vulnerabilities, and risk managers will be needed to help train employees on how to handle company assets responsibly in their everyday tasks.

Operationally, such a shift in mindset towards a holistic and proactive approach to corporate security will likely come (at least in part) from the top down, making individuals with experience in c-suite positions like CISOs, CIOs, CEOs and especially CSOs or COOs absolutely essential.

Experienced managers, especially those familiar with procedural-, operational-, and especially business continuity- management will also be a considerable asset to companies looking for security scouts.

For now, there is no single well-defined course of study for individuals hoping to become ICS professionals. However, certificates and qualifications like the HWZ’s CAS in Business Protection provide ambitious individuals with a firm foundation in holistic approaches to corporate security.

Personality:

Besides technical know-how, there are several key personality traits that will contribute to the success of candidacies and careers in security scouting. Curiosity, quick lateral thinking, pragmatism, strong analytical skills, and an investigative streak are all crucial for a successful career in ICS. In addition, the ability to efficiently translate theory into practice and a propensity for seeing thing’s from an opponent’s perspective are also increasingly important.

“We need individuals with a talent for holistic problem solving who can persistently think through challenges and threats from all angles, and we need lateral thinkers with the courage to challenge superiors when they see that ICS best practices are not being adhered to”, says Chris. “Believe little, question everything, and always think for yourself”, this is the creed that successful security scouts of tomorrow will live by.

ICS is, by definition, a team effort – threats are always changing and no one person will have all the necessary qualities to ensure impenetrable corporate security. It is therefore crucial that aspiring ICS security scouts are able to network and integrate well with others in an ever-changing environment – joining forces with individuals from diverse backgrounds to identify and tackle vulnerabilities in a business from all angles.

In conclusion, as Peter Kosel, Founder and Talent Community Manager of cyberunity AG, points out, the future of corporate security essentially depends on three developments: First, businesses and their executives will need to recognize the value of awareness and ICS. Second, they will need to establish forward-looking talent pools composed of diverse, dynamic, and capable individuals (rather than sticking to the conventional recruitment process which only starts once a vacancy urgently needs to be filled – KNOW YOUR TALENTS). Finally, such diverse, dynamic, and capable individuals will need to recognize the value that they can add to such businesses and step up to the plate.

Those interested in the CAS in Business Protection starting in June 2021 can find more information and register for the course via the following link:

Registration **CAS Business Protection**