Image by Susanne Jutzeler via https://pixabay.com/photo-3632278/ (copyright-free)

Decoding Cybersecurity: Interview Insights with Leaders Pt. II

Elliot Marshall
Security Operations Executive | Financial Services Security Strategist | Enterprise Security Transformation | Trusted...

February 19, 2019

Throughout 2019, this mini-series will interview leaders from around the globe to discuss areas of cybersecurity. The purpose is to help students or those new to the industry gain perspective and guidance from professionals in the field. These interview insights aim to kick-start or re-energise your career journey in cybersecurity.

In this month's feature, **Justin Greis**, EY's Americas Practice leader for Cyber Resilience, shares:

- His description of cyber resilience, and how this is portrayed in the market.
- What, if any, information would he have liked to know starting out in his career.
- How he suggests others new to the field get involved.

Greis describes how he discovered his passion to tinker and build things early in his career, which fostered his love for technology and business. He loved the

idea that technology could fundamentally make lives better, more efficient, and more enjoyable. His career journey spans as an entrepreneur owning a technology consulting company to EY where he has gained experiences across a full spectrum of Advisory services, including Cybersecurity. His professional journey has led to many opportunities across technology to help his clients solve their most complex business and technology problems.

These are his insights.

What is cybersecurity resilience, and how this is portrayed in the market?

Greis outlines concerns he hears from the Boards he consistently interacts with where cybersecurity risks are the number one concern. Greis questions, “why are we seeing an increase in public attacks that make headlines? Why are these attacks becoming more destructive and manipulative? We saw this wave of events turning away from fraud, exfiltration and manipulation from people and blackmail to destruction and now, more broadly, cognitive warfare shaping our social and political discourse. Our team decided to address these challenges. We defined Cyber Resilience as an organisation’s ability to prepare for, respond to and recover from a cybersecurity-triggered business disaster - which we characterise as a large-scale cybersecurity-attack with the intent to destroy or manipulate critical data or systems.

We analysed leading companies and established a hypothesis that there is often a missing discipline in a cybersecurity function that focuses on the capabilities that enable a company to defend and adequately recover from disaster-level attacks. We defined this capability into Proactive and Reactive elements.”

The Proactive function is the 'running' aspect of Cyber Resilience. Security Architecture is, so often a missing discipline, and Greis believes it is an essential component enabling a company to bounce back. Greis explains, “security architects develop resilient patterns of cybersecurity solutions that are propagated, evangelised and promoted throughout the organisation. These patterns can be taken from prior attacks, natural improvements and upgrades, or can arise out of proactive investment to improve the cybersecurity posture of an organisation.

The Reactive function activates when a cybersecurity-triggered business disaster occurs. We identified that a discipline called Cyber Crisis Management (CCM) is often missing from the equation. We found too often when an incident occurs it is:

- The Security Operations Centre (SOC) or Incident Management (IM) Commander taking control and getting 'quickly out over their skis';
- The Crisis Management (CM) team, whom are communications experts, but limited in their capability to command and control a situation or navigate technical remediation; or
- The Disaster Recovery (DR) or Business Continuity (BC) team, whom may unintentionally cover up or even worsen the incident to restore availability of compromised systems."

Greis describes, "this CCM function is intended to serve as the hand-off point between the SOC and IR, and

- handle the crisis as it occurs;
- manage remediation;
- initiate reporting; and
- serve as the command and control function."

Greis emphasises, "we believe this is a critical component of Cyber Resilience and should live in the Cyber Crisis Command Centre (C4); an area we do not typically see defined in maturing organisations early in their cybersecurity journey. However, in leading organisations within the technology, financial, or critical infrastructure (such as power and utilities) sectors for example, there are established C4 functions out of necessity because it is mission critical to serving their customers. We view this as an opportunity to help our clients better prepare for, respond to, and recover from a cybersecurity-triggered business disaster."

What, if any, information you would have liked to know starting out in your career?

Greis explains, "I would categorise the advice and guidance into three buckets:

- **Learn to say 'No' graciously.** In the early part of my career, I always felt it was impossible to say 'no,' and I think this is a fallacy and misperception by junior people because they do not want to disappoint their colleagues and bosses. What I did was work when I had downtime or in my free-time as I felt, like many others, I had to prove myself. Granted, at EY if you work hard and did quality work for your clients, people will notice, and this will pay off; however, I wish I would have learned that it was OK to say 'No' a little earlier on. I put a lot of pressure on myself, but it turned out that it was all in my head and it was OK – and even expected – to turn things down…in a nice way, of course.
- **Do not underestimate your experiences.** Any career moves you make are only temporary. I see a lot of young people feel like when they enter a new career or start a new job that they will be stuck in that role and profession for the rest of their lives; rather there is value in the culmination of our collective career experiences. The diversity of my background has enabled me to be a better consultant and see things from multiple angles. We are the compilation of our experiences rather than a single role at one point in time. I remember early on I found out I did not have a passion for doing only audits. I remember the panic as I did not know if I would have a role or career at EY. I am thankful for the great mentors and leaders whom helped guide me and set me on the consulting and advisory path. It Is Okay to try different things; you become a better, more well-rounded professional as you obtain broader experiences over your career.
- **Enjoy the journey.** Take time to enjoy the journey that you are on. Take time make friends with the people you work with. They can be the some of the best friends and most wonderful people who can fundamentally shape you and your life. The network and relationships we build are critical for your career advancement and personal well-being. Also, find time for hobbies, your personal interests and the things that pique your curiosity. Free time seems to decrease as you get older but you can always find time for things you make a priority."

How would you suggest others new to the field get involved?

Greis emphasises, "This is similar advice I provide to anyone attempting to make a career switch; it has never been easier to reinvent yourself in today's technology-connected world. If you are in the consulting space, you can become whatever you want to become. It just takes effort and initiative:

- **Be your own pilot.** You can learn about resilience via a variety of mediums (training, classes, certifications, blogs, YouTube, publications, books).
- **Activate your network.** Network internally within your company, and externally as part of professional organisations to better transform into a Cyber Resilience professional. People come from various backgrounds and there is no single path to entry. Find the path that works best for you, but keep in mind this will take effort.
- **Develop the fundamentals.** If learning the fundamentals is needed because your background is not IT related, there is always higher education to facilitate the development of resilience skills and knowledge. If you have transferable skills, it is not difficult to make the transition with a little elbow grease. And do not forget to look within your own organisation and volunteer for projects, activities or 'extra curriculars' that are closer aligned to the career direction you want to go."

In conclusion, this month's edition was supported by **Justin Greis**, EY's Americas Partner and Practice Leader for Cyber Resilience, where he:

- provided insights into his professional journey;
- detailed the future of cyber resilience;
- expanded upon three career-starting tips (Learn to say 'No' graciously, Do not underestimate your experiences, Enjoy the journey); and
- emphasised three approaches to get involved (Be your own pilot, Activate your network, Develop the fundamentals).

This area of cybersecurity is intriguing, in-demand by the market and considered as an excellent career starter.

Please be on the lookout for next month's issue of *Decoding Cybersecurity: Interview Insights with Leaders* as the journey continues.

Please leverage the comment box below to suggest future topics, recommend guests, provide feedback or share with others.

Check out the January 2019 edition with Alexandra Panaretos, EY's Americas Practice Leader for Cybersecurity Training and Awareness.

Check out the March 2019 edition with Shane Moffitt, the Assistant Chief Information Security Officer (CISO) for the Victorian Government.

Check out the April 2019 edition with Brian Kelly, Chief Security Officer of Rackspace.

Check out the May 2019 edition with Aaron Johnson, Global Cybersecurity Governance, Risk Management and Compliance leader at Dana Incorporated.