BRINGING RIGOUR TO SECURITY: HOW HARD COULD THAT BE?

A STORY BY SIMON SHIU

RISCS Research Institute for Sociotechnical Cyber Security

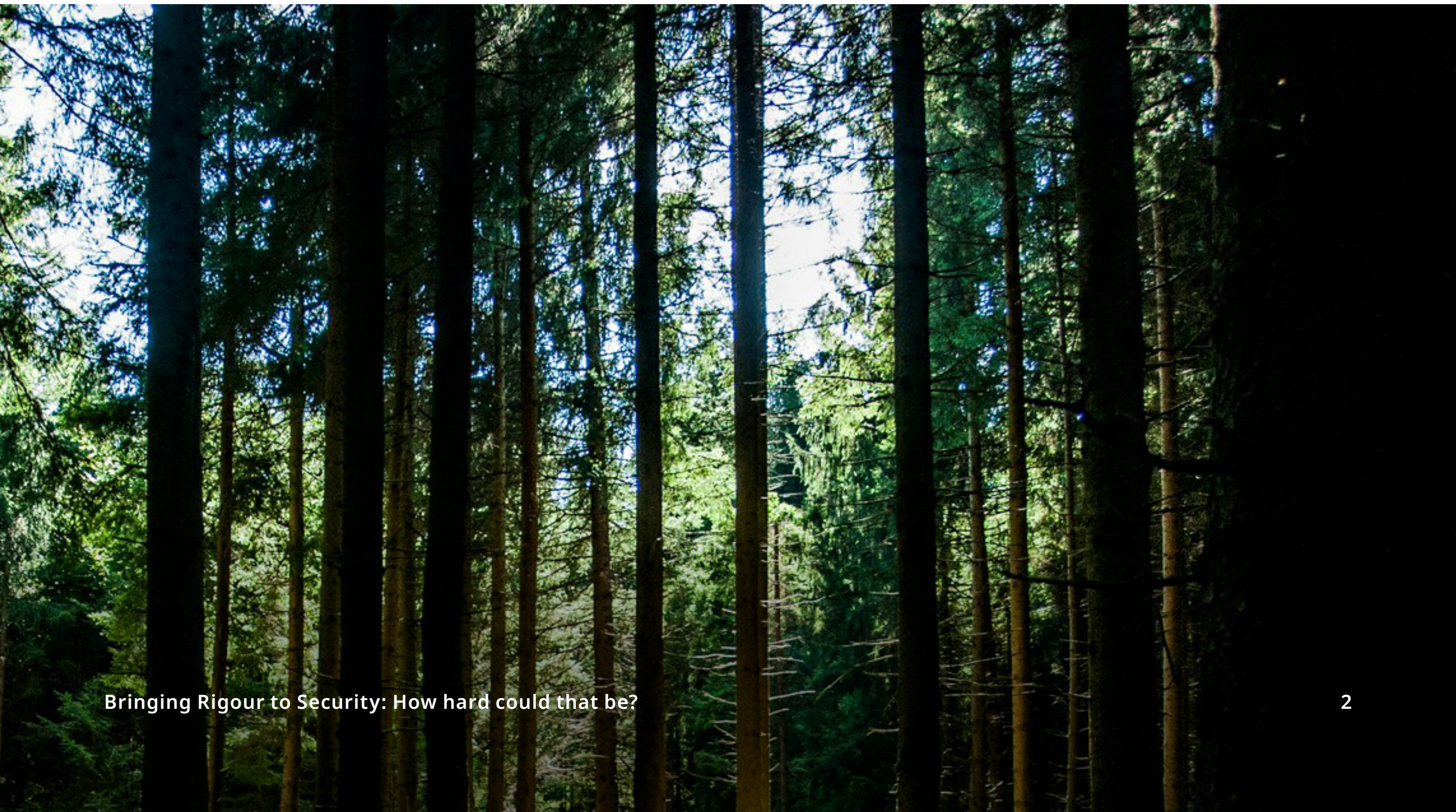
Monday, Roger the new starter meets Cal the CISO

Cal had liked the CFO’s suggestion she bring an accountant into her security team. The business was innovating with social media and expanding digital services; she needed allies if she were to keep ahead of the risks. Gaining an insider that could help articulate business risk in finance terms seemed a smart move.

As Roger shook Cal’s hand she noticed him glance hesitantly at the two available chairs. Looking for a way to break the formality, she suggested a walk across the tree-lined campus and invited Roger to share his initial thoughts on his new role.

She liked how he phrased things in business terms; and was impressed that he covered a lot of ground from security operations to culture. He humbly acknowledged he had a long way to go to *“see the wood for the trees”* never mind map this to financial risk. She held back from explaining that the forest itself is constantly changing, with emerging technology continually disrupting the business and threat environment.

Cal felt she could read people, and, like a good poker hand, Roger had potential. She encouraged him as he talked naively about doing a quick survey of the security market, so he could *“provide a more structured return on investment analysis”*. As they reached her office a confident Roger asserted *“I’ll start online, let’s check in tomorrow”*.



Tuesday, Roger has Coffee with Frank the Security Salesman

Is it deepfakes that will undermine the election? Roger loosened his tie and feigned concentration as he struggled to follow the conversation with Frank. And it's quantum that will break all banking transactions? OK. So, what is it spearfishing and ransomware do?

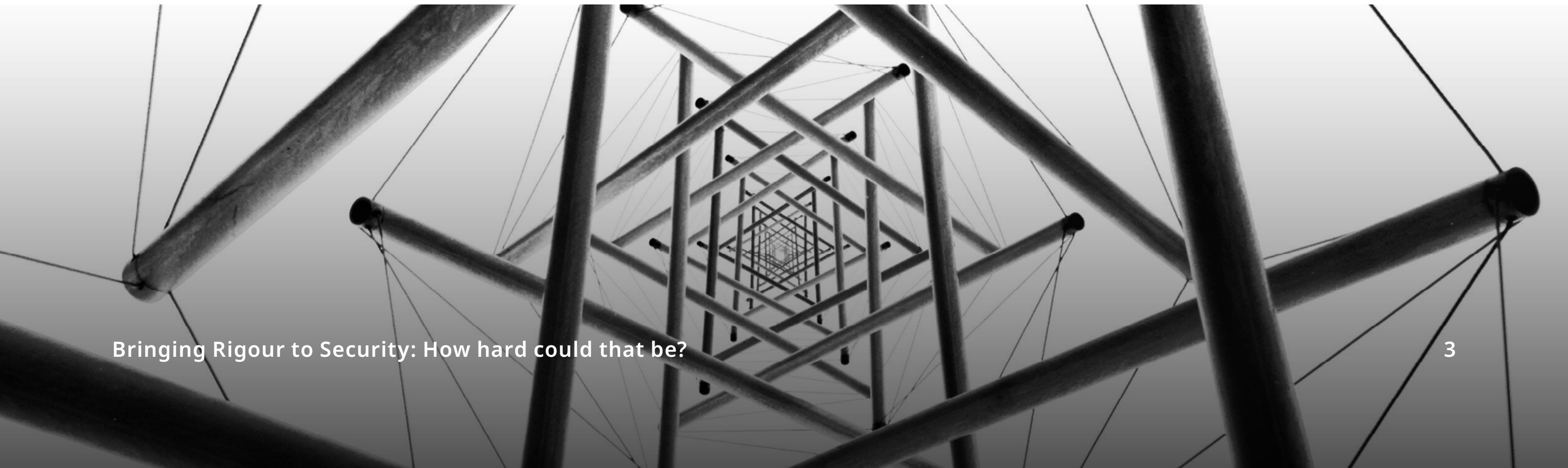
Only yesterday life seemed simple. Cal the CISO, his new boss, had been friendly and open to his ideas for bringing accounting rigour to cyber management. Keen to impress he had started browsing for security products that best address business risk.

He was quickly spooked by the number of digital catastrophe stories online – especially those involving finance teams approving astronomically large payments. He clicked on, and grew more wary, feeling like he was in a medieval bazaar, with shiny security products being offered by doomsayers and snake charmers. It was somewhat a relief when his old colleague Frank messaged him on social media. Frank must have seen he'd adjusted his profile from accountant to cyber security analyst – and that they were now working on the same campus.

They met over coffee and at first Frank's explanations had been helpful. Roger knew about firewalls and anti-virus, and with these footholds he felt more grounded. One tree at a time he reminded himself. As his mind wandered, he saw himself impressing Cal with an insightful overview that mapped products to risks mitigated.

But he was soon finding it hard to see the wood for the trees. Firewalls and anti-virus tools were just the start in protection and detection products. The security tree soon branched into signature and behavioural detection, email gateways, intrusion prevention and more. Then Frank was pointing to other 'trees' like identity management, resilience, privacy, and compliance.

Sensing that Frank was building to a commercial proposition and knowing he wasn't equipped to make any calls, Roger thanked him and said he'd sleep on it.



Wednesday, Roger has dinner with Irving the Industry Analyst

Roger’s head was spinning again, but this time because of the rather good Shiraz that was generously being refilled into his glass. Cal had recommended Roger spend some time with Irving Adams, *“an old friend from the world of industry analysts”* – someone that can help you *“navigate the forest”*. And Irving was easy to follow, making security procurement seem more like browsing a department store. Security products were arranged into sections and differentiated by vendor maturity, vision and execution. He was beginning to see how to compare endpoint security, security monitoring and application security vendors.

Irving leant back, from his well-rehearsed delivery and poured some wine.

Collecting his thoughts Roger said, *“the categorization helps, but how do we figure out if a product is right for us”*.

“It’s a good question, and don’t forget security is about much more than the products”.

“What does that mean?”, Roger asked.

“Well products have to fit into processes, and all this sits on your cloud and endpoint infrastructure, which are the foundations that set the rules for security”.

Roger looked sceptical, so Irving expanded, *“think about it, a large organisation has thousands of mobile devices accessing hundreds of applications on global cloud services; this infrastructure determines what security products and operations are needed”*.

“Ok, I get it” said Roger, *“The CISO isn’t the only stakeholder here. Cal needs to influence how IT build security into the business”*.

“Right” Irving confirmed.

“It seems pretty hard for vendors, trying to second guess customer preferences then!”

“Yes, but conversely the customer has a hard time assessing the security design and quality of vendor products.” Irving said. *“So, I wish the economists luck applying their theories to our market”*.

As they split the bill, Irving added that his ‘analysts view’ was very commercial, and perhaps should be balanced with a view from a technologist.

Thursday, Roger in the Lab with Georgia the deep technologist

Roger regretted saying he was good with numbers. It seemed a way out of discussing attack trees and penetration testing, but now his techie friend Georgia was enthusiastically describing trapdoor functions and randomness. These bizarre branches of mathematics bore no relation to balancing books but were, apparently, relevant to making cryptography *“one area of cyber security with strong theoretical foundations”*.

He hadn’t seen Georgia Haycroft since university, but he recalled she had grown up fixing and breaking games consoles and other electronics. She didn’t wear a hoodie, but her work environment was considerably more casual than he was used to. Armed with degrees in electronic engineering and cryptography, Georgia made a living *“certifying products for ‘good’ security”*.

This seemed to be about taking a product fully apart, seeing how it was made, what it was designed to do, and how to be sure it couldn’t do things it wasn’t intended to do

So, it made sense that the market would use specialists like Georgia to independently certify that a product is ‘secure’.

“You’d think so wouldn’t you” sighed Georgia. *“And we do a lot of work certifying security products with well understood theory and standards – like gateways and cryptography”*.

At this point, the previously inert youth with his head focused on his monitor piped up *“the reality is, labs like these are expensive to run, the assurance process is painstakingly long, and the infrastructure is expensive”*.

Seeing confusion on Roger’s face, Georgia introduced Chris, *“a PhD student interning in our lab”*.

Chris carried on *“Most vendors need to get a product to market, and not many customers have time to specify all the security properties they need from a product, so the idea of waiting for a certification is, let’s say, commercially challenging”*.

This led to an engaged discussion on how a vendor could establish technical and market credentials for their products. Chris explained, *“most standards, even if they are measurable or auditable become ‘the lowest common denominator’”*. That seemed a strong statement to Roger, but he was persuaded that doing more seems to require companies to take a long-term strategic view, investing in innovation, messaging and industry leadership.

Still Roger came away enthused that there were experts analysing what ‘good’ security looks like. It seemed different from but related to, the market analysis of Irving – surely there are ways to join the dots between these worlds.

Friday, Cal and Roger reflect on the learning journey

"The market analysis is great, but surely, we should be using more of the scientific and engineering principles to say what 'good' security looks like?".

Cal smiled, as Roger expressed a philosophical question that regularly piqued her interest. Piqued but rarely indulged she sighed. But who was she kidding, her passion was to transform the risk culture of the organisation. The CEO and CFO were on board with this. Most of the business and IT leaders were too, although as individuals it was harder to get time with them. No doubt they assumed her inputs would jeopardise their investments with pesky concerns about risk and governance.

Also nagging at the back of her mind was the quarterly board presentation that she was due to deliver next week. At the last board meeting, the board had channelled their inner *"dragons' den"* and spent more time sharing their knowledge of AI, geopolitical risk and regulations than engaging with her plan to bring more rigour to cyber risk governance.

She must make time to be ahead of all the conversations and headlines the board will be absorbing. This is why she keeps up her external network, and why Irving and his like, hold so much influence. Setting the agenda at industry events, framing customer problems and judging vendor solutions; they set the narrative for what gets attention and early dibs on the prevailing perspectives.

Cal thought it might be good to road test her risk pitch with Roger. But snapping back to the conversation she heard Roger opine *"We need to do more to tap into all the research; from designing for humans and economics to computer architecture and software engineering"*.

"I agree", she declared, *"However, it is not easy to interpret this evolving body of knowledge"*.

Finishing her coffee with Roger she reflected, the best thing about this week was that she'd recruited a fellow traveller on this journey.