RISK LEDGER

NOVEMBER 2023

DEFEND AS ONE:

THE CASE FOR COLLABORATION IN DEFENDING AGAINST CYBER ATTACKS

HAYDN BROOKS

If you want to beat the bad guy, you're going to need a whole community of good guys on your side. In other words – when it comes to cyber security – collaboration is key.

"With great power comes great responsibility," said Uncle Ben to Peter Parker (or Spiderman as he's more commonly known). And Uncle Ben was right, of course. Beating the bad guys by yourself is a heavy weight to bear on even the most powerful of shoulders.

So why do we expect single organisations to have the capacity and expertise for fending off cyber criminals alone? Why, when an organisation comes under attack, are we so quick to blame them for having ineffective security controls instead of looking at the bigger picture?

Organisations are linked, whether they like it or not, and the responsibility for preventing cyber crime is inescapably shared by the entire ecosystem. Blaming a single organisation for falling victim to a breach only perpetuates an every-man-for-himself mindset which does nothing to stop further attacks. To put it simply, an organisation's defences are only as strong as those of the other organisations in the ecosystem, so sharing resources and data is in everyone's best interests.

Sure Spiderman did some great things in New York single-handed, but when the planet needed defending from the most powerful threats in the universe, it was The Avengers who stood together as the first line of defence. And so, when it comes to defending against cyber attacks, collaboration between organisations is vital.

What are organisations doing wrong?

For most organisations, cyber security isn't the main priority. How can it be? If you walked into the headquarters of a large supermarket chain, Tesco for example, and asked ten different people what the company priority is, surely they would say "getting products into the hands of our customers".

If you walked into the headquarters of an organised crime group, however, you'd come face-to-face with a team whose number one priority is to carry out cyber attacks. Even script kiddies – who may not have the most sophisticated techniques – have one thing that organisations lack: time. Their sole aim is to find something to break. And they will find it.

How can we expect a single organisation (the solo warrior in this analogy) to compete against whole teams of cyber criminals (the bad guys) who spend their time on nothing else but figuring out new ways to bring organisations to their knees? In truth, we can't actually expect individual organisations to build and maintain cyber defences

and keep out determined attackers. It simply doesn't make sense.

So what is an organisation lacking in the capacity and expertise for security to do? Many turn to outsourcing – which is much better than doing nothing – but it doesn't solve the whole problem. Outsourcing is only part of the solution because adopting any of the most common outsourcing models currently available still leaves organisations with the same obstacle: they can't outsource responsibility.

Security providers have a defined scope, a clear contract, which means they're only incentivised to deliver exactly what the organisation has asked for. Nothing more, nothing less. An outsourced provider isn't going to step back and look at the holistic, contextual risk to an organisation. Sure, organisations can hire consultants but it's far too expensive to be sustainable long-term.

Clearly what organisations are doing to defend against cyber attacks isn't working; attacks are increasing. We need to work smarter, and that starts with working together. Organisations have no choice but to lean on each other's strengths and see all weaknesses as collective in order to defend against cyber crime.

How can organisations do it right?

The solution is simple: organisations must collaborate with their connections; from suppliers and clients to every commercial and strategic partner in their ecosystem. Just as The Avengers joined forces to defeat common enemies, so organisations need to think of themselves as an interlinked community working together to defend against cyber crime.

Connected organisations have a natural incentive to make sure there isn't a breach within their ecosystem. When everyone is connected, an attack on one organisation is tantamount to an attack on every organisation, which means that looking out for each other can only be beneficial. And conversely, failing to collaborate can only be detrimental for everyone involved. Organisations with large security operations centres and strong expertise in hunting, detecting and responding to attacks must rally around their smaller partners and suppliers in order to protect the whole system. When it comes to cyber security, organisations can only win when they play as a team.

Criminal groups use particular tactics, techniques and procedures (TTPs) that help organisations identify them and predict their next move.

Analysing these patterns is significantly more useful on a large scale but detection and response tooling is typically deployed within the confines of one organisation. We all know the power of big data – we've seen what Google or Facebook analytics can do. Now imagine the power of every connected organisation analysing their network traffic, endpoint device activity and cloud service provider logs at scale – then sharing attack analytics data with their entire ecosphere.

Legally, of course, organisations will need to maintain the same protections and continue to segregate responsibility, but technically, these divisions are now much more blurred. Organisations no longer have a defined perimeter. If they want to defend themselves against cyber criminals, they'll have to actively prevent cyber attacks against every connected organisation in their network. Legal boundaries won't stop attackers, but taking collective responsibility for cyber security within an ecosphere just might.

Are cyber attacks really such a big problem?

In short, yes. Gone are the days where you had a distinct line in the sand between organisations who were digital and those that weren't. At this point in our history, all organisations are digital. And with that rapid increase in digital adoption, the incidence of cyber breaches is increasing just as fast - despite the best efforts of security professionals, IT teams and business leaders.

Will organisations be willing to collaborate?

From what we've learned over the past three years at Risk Ledger, the answer is yes. Every day we see suppliers being more honest and transparent about where they're lacking in security controls – and their clients taking practical steps to help them improve. With access to a platform that makes collaboration easy, we've watched organisations go out of their way to shore up security defences across the whole supply chain as a team, instead of simply cutting ties with weaker links.

Risk Ledger uses a social network model which means that a map of the global supply chain is constantly building in the background; connecting security teams who can engage with each other and collaborate on improving security controls. This network of connected organisations provides the backbone upon which to build a true collective cyber security defence system where all organisations defend as one.

And while we don't expect to see the organisations connected through Risk Ledger becoming "the planet's first line of defence against the most powerful threats in the universe", we can already see their collaboration becoming the global supply chain's first line of defence against cyber attacks.

HAYDN BROOKS

Co-founder and CEO
Risk Ledger

Originally a big 4 cyber risk consultant, Haydn experienced the day to day issues that came with running a supply chain assurance programme. He found that current programmes were far from frictionless and actively caused clients and their suppliers' headaches.

These pain points led him to found Risk Ledger. Risk Ledger is a technology platform that combines a security governance platform with a secure social network.

In the last couple of years, Risk Ledger has gone from strength to strength, receiving 2.1 million in seed funding, winning the Cyber Den/Most Innovative Cyber Company Award and being named as one of Forbes' Tech Champions of 2022. In addition, Haydn was featured on the Forbes 30 under 30 list.

What is Risk Ledger?

Risk Ledger is a supply chain security platform based on the model of a social network.

- Get the right risk assessment data with our dynamic controls framework. It unlocks network effects to scale your supply chain security.
- See live assessment data in supplier-owned profiles (like Linkedin for cybersecurity).
- Send and receive updates about controls in real time. Our network model means suppliers and clients are always connected.
- Collaborate on remediation and other tasks directly in the platform.
- Visualise concentration risk beyond third parties.
- Do continuous monitoring, but from inside out.
- Join us in creating the future of Defend-as-One. (No organisation is an island. Already, many customers use Risk Ledger as both a client and a supplier.)

GET IN TOUCH