Episode Three:

We're All Human, We're All Vulnerable

HOW EMERGING CYBER THREATS POSE NEW CONTINUITY CHALLENGES.

POWERED BY:

Databarracks

BCP

Historically, cyber security and business continuity have been adjacent, but separate activities.

However, as cybercrime develops into a multi-billion dollar industry, the growing frequency, sophistication and disruption of attacks increasingly fulfil conventional disaster criteria. So what that mean for the many already overworked continuity professionals for whom cyber has suddenly become a core concern?

Cybercrime is big business

Cybercrime is evolving at a staggering pace. The variety of threat actors today (and their chosen methods) are unrecognisable from the bedroom-based, lone actor stereotypes of just over a decade ago.

Highly regimented criminal organisations are employing talented technical professionals to access and exploit privileged systems and data, whilst isolated threat actors enjoy easy access to sophisticated malware that's affordable and easy-to-use.

A policy paper released by the UK government in 2015 revealed that 81% of large corporations and 60% of small businesses reported some form of cyber breach in 2014.

For Vicky Gavin, Head of Business Continuity and Information Security at the Economist, we're witnessing the rise of one of history's great criminal developments.

"I actually compare cyber-crime to prohibition, in terms of the way it's increasing. Organised crime see this as a huge money-maker. There are people whose job it is to steal data, and they do this 24/7/365. Most of us on the other side, it's not the only thing we're doing. And as long as that inequality exists, it's quite lucrative for the criminals to keep stealing stuff. They get a good return on investment. The level that they have to attack at is not huge. And I think the biggest factor is prosecuting them is really difficult. So there is some level of impunity there that they're taking advantage of."

Cyber has become a continuity problem

Cyber capabilities evolve on a continual basis, and new threats emerge all the time. It's growing fast, and everyone is trying to catch up - from security teams, to continuity professionals, to law-makers.

And like so much of the traditional complexity around BC and DR, the main challenge is variety. Different kinds of threats, different perpetrators, different technologies, different methods, different objectives. It's all contained under the cyber label, and that variety makes it very hard to keep continuity planning as localised and specific as possible.

Nevertheless, Matt Hogan of the London Fire Brigade urges people to take an interest in cyber, even if it's outside their typical remit, if only because its effects can be so far reaching.

"There's lots of talk about cyber in the media, but...

"...within that cyber bucket there's lots of different cyber risks."

There's not a one size fits all solution for cyber. So there's the hacking, phishing, fraudulent element of cyber - our team doesn't deal with that, the police and security do. But there is also the potential for cyber to affect infrastructure systems, to attain data that allows you to implement a traditional attack, and I think we need to better understand that cyber risk environment to understand how to treat it."

Cyber methods are outpacing security innovations

It's not just organised crime groups for whom cyber is big business. Worldwide spending on information security reached 75 billion dollars in 2015, and analysts are predicting it'll reach 170 billion by 2020.

The trouble is that traditional, software-based methods of anticipating and preventing cyber-attacks are struggling to keep pace with the more closely targeted, social engineering strategies of modern attackers.

Most attacks today don't involve any brute force activity at all – instead relying on legitimate credentials, illicitly obtained from an often forgotten source of risk: unwitting users. The capabilities of expensive security products are therefore mis-aligned with the most common and most serious cyber threats.

For Rob Dartnall, Director of Cyber Intelligence at Security Alliance, a lot of it is technology overkill. He advocates a different, intelligence-based approach.

"When I first came into cyber I generally found there were a lot of vendors doing stuff that was very unspecific to a problem. A lot of it was marketing companies putting nice spins on sexy words. Intelligence is a hugely misused word in the industry that a lot of vendors have picked up on, put on their marketing material, and sold extremely expensive, seven figure products on the back of it.

"However, we've certainly noticed, over the last six months that intelligence, because of the importance of it, is being picked up. People are starting to design products that are properly intelligence-based and use proper intelligence methodologies, rather than just the term 'intelligence'."

Everyone is becoming more intelligence-based

Whether they misuse the term or not, 'intelligence' products are becoming more popular for a reason – the instruments of attack have never been so powerful and yet so easy to acquire and simple to use. It seems like an arms race. Rob Dartnall commented on the apparent arms race between attackers and their targets.

"Everyone has stepped up their game."

"Low level attackers now have access to quite high level and sophisticated toolsets. Some of these pieces of malware come with user interface GUIs, so they're really easy, and propagating malware all over the place.

"Individual and organized groups don't even have to buy malware products any more – they can now rent it for a number of hours. They can rent botnets. It's a business, and there's a lot of conventional businesses and industries that could probably learn from the speed at which the dark web is propagating its wares.

"On the other side of things, organised criminal gangs are working with quite large budgets, so they are able to buy talented software and malware engineers, and manipulate existing (or create new) malware for their own uses."

Truly organised crime

It's easy to underestimate a phrase like "cyber-crime is big business", and understand it only in financial terms. Operationally speaking, successful organised crime groups share countless parallels with successful legitimate enterprise. These are disciplined, strategically managed businesses working across sophisticated global infrastructure. Rob Dartnall outlined the scale of many criminal organisations.

"Organised crime in cyber is huge, we're talking billions and billions of pounds a year..."

"...and it will only continue to get bigger. As they get bigger they earn more money, and as they earn more money, they become more sophisticated, so it's a perpetual motion for them.

"We're not talking your friendly hacker sending you a phishing email about their cousin who has got £400m in an offshore account but needs some money to help it come back into the country, you're talking about highly sophisticated malware engineers, and highly sophisticated business people.

"There is one particular group that are actually known as 'The Business Club', or the 'Evil Corp' as they're also known, and they run themselves as a business. They have marketing and PR and accounts and finance, and all of the different business functions. They got their name because they run it like a business and they make a lot of money from doing it."

Next to Vicki Gavin's allusion to prohibition, Rob's account of cyber criminals seemed clinical, and emotionless. There was no malice towards their targets, no aggression in their attacks. With the exception of political activism, most attacks seem transactional – quite literally just business.

What can organisations do?

As we've seen, incorporating cyber security into your continuity plans isn't just a matter of spending more money on software solutions. The most valuable element of cyber resilience is not technology, but education.

A basic understanding of some cyber intelligence fundamentals will significantly improve your ability to both identify your vulnerabilities, and enact behavioural changes at the user level that cumulatively amount to a very credible level of security.

First: the Attack Surface.

Your overall attack surface is the sum of the individual attack vectors through which you are vulnerable to attack. That might mean technology blind spots, physical points of entry, or high value individuals such as senior executives or administrators with privileged credentials.

As Rob Dartnall explained, mapping out your possible attack vectors in order to understand your overall attack surface isn't a new idea.

"A lot of older intelligence methodologies are ancient concepts, tried and tested over centuries.Sun Tzu was talking about intelligence a very, very long time ago, in terms of understanding yourself and the enemy.

"That's completely transferable to today's environment."

"For instance, if you're talking about how an adversary on your network is going to come at you, you might design an attack tree that will show all of the different stages that they will have to go down in order to get to your critical asset."

What can Backcasting do?

Next, Rob Dartnall also spoke of the value of Backcasting as a means of quantifying hypothetical aspects of risk by starting with an incident and working backwards, ascribing clear drivers to every stage.

“Working backwards is a methodology that I strongly recommend.”

“A Backcasting exercise is what’s known in the intelligence industry as looking at an end point, working backwards and seeing all of the things that have to happen in order to reach that end point. From that you will start identifying signposts, or signals that you know, ‘If you see this, then it is likely this is what is going to happen, and if this happens, this is the consequence of that.’

“So start with your critical assets, major commercial risks and most important business areas, identify worst case scenarios for them, and work backwards until you reach business and usual again.”

The Cone of Plausibility

The Cone of Plausibility is another planning exercise that encourages users to plan with a degree of flexibility by demonstrating how small, unexpected deviations in circumstances can radically change the outcome of an incident.

“The cone of plausibility takes a given scenario and tweaks small elements of key drivers in order to observe the different possible outcomes from similar initial conditions.

“Cones of plausibility are valuable because they broaden your understanding of different drivers and how they impact ultimate consequences. Small variations often yield major differences.”

The Tenth Man

Whilst we’re a strong advocate of simplicity in continuity planning, things can quickly and unintentionally become complex.

Rob Dartnall’s ‘Tenth Man’ isn’t an individual planning exercise so much as a failsafe mechanism that highlights any blind spots by bringing in an outsider to interrogate your plan.

Someone with no context of your prior discussions (and sometimes even subject matter knowledge) will often provide a fresh perspective to the topic, and ask questions that may have been overlooked.

"The secret to intelligence, if there is any secret to intelligence, is just good people, in a room, with a whiteboard and a pen. I incorporate a methodology called the Tenth Man – somebody who comes in with no prior knowledge of what you've been discussing, and – mostly unwittingly – tears your work apart.

"That's why it's always important to have outside influences. If you're coming up with scenarios, cones of plausibility, hypotheses etc., it should not be one person left by themselves. It should be the different business owners sitting in a room with a whiteboard."

What can organisations do?

Users are far and away one of the largest and most vulnerable attack vectors for organisations. However, it's also one of the most easily remedied. User education is a huge component in becoming more resilient against social engineering programmes. Showing users how to spot spear phishing emails, and what to do when they receive one (send it to security and delete it locally) is a simple but incredibly effective defence, as Vicki Gavin of the Economist attested to.

"Spear phishing isn't always necessarily just one compromise, if you like."

"When somebody has an internal foothold, it's quite possible for them to start spoofing an individual's email, or using that email account that they've already got in.

"When you've got a company of 20,000 employees, every single day within your organisation somebody will click on something, 90% of the time your natural defences will pick up on these things, your IDS systems or your IPS systems, but it's the ones that get through, that's where the pain starts."

However, engaging users in a meaningful way that results in long term behavioural change is easier said than done.

Vicky Gavin's Security Blanket exercise gamified the process of identifying spear phishing emails and reporting them to IT to great effect.

"October is Security Awareness Month, and one year we ran a "phishing contest": for everybody who sent us a phishing email, we gave them a raffle ticket for a beautiful, handmade 'Security Blanket'. It really incentivised people to identify phishing emails for five weeks.

"All of the behaviourists will tell you it takes three weeks to form a new habit. So if I get people to do something for five weeks, they've pretty much formed a new habit and can now identify phishing emails pretty reliably."

There are a lot of parallels between cyber and continuity planning, not least because neither need to be complicated to be effective – a little effort goes a long way. Exercises like the attack surface, back-casting and the cone of plausibility are great ways to think about risk, resilience and continuity from a different perspective.

However, as Rob Dartnall of Security Alliance was keen to emphasise, your plans should stay current, and reflect the external risk landscape as it evolves.

"Honestly, there is so much information out there now...

"...a simple Google search is all you need to find it."

Although a lot of intelligence information is from closed sources, there are a lot of organisations that write incredibly informative white papers and press releases, and a lot of good guys who work in cyber security who keep worthwhile blogs.

"For instance, we know that in the Ukraine, it's quite openly reported that the predominant malware is Black Energy 3. So if you happen to be a Chief Information Security Officer at a piece of critical infrastructure that looks a little bit like a Ukrainian electrical distribution centre, then you need to start looking at Black Energy 3 – what it does, how it does it, and how you protect yourself against it.

"So yes, actually just Googling your industry peers along with some attack-based keywords and keeping up with the daily news feed, is a really basic, but effective way to stay prepared."