Threat intelligence: why people don't share

Tim Ring

Tim Ring, freelance journalist

One tube-strike morning in early February 2014, the UK Government's Business Secretary Vince Cable called a summit of government ministers, senior intelligence officers, and finance, power, telecoms and transport industry regulators, to take action against the "serious and growing" cyber threat to UK plc.

One of their main recommendations was the need for more information-sharing on cyber-attacks. All well and good. But a much more powerful argument came a few days later with the discovery of the 'Mask' APT attack which had infiltrated over 100 UK government, critical infrastructure, finance and other systems, and whose Spanish-language signature pointed to a new 'threat actor' on the global stage, beyond the usual suspects of China and the Russian region.

This was dramatic backing for Vince Cable's recognition that the cyber threat is radically growing and changing. The feeling is that resistance is almost futile – it's a matter of when not if you will get breached, and serious attacks typically go unnoticed for months if not years. So it's not enough just to throw security technology around the perimeter of the organisation – these days, enterprises need to gather and share real-time intelligence on new cyber threats, to either prevent attacks happening or at least quickly recover from them.

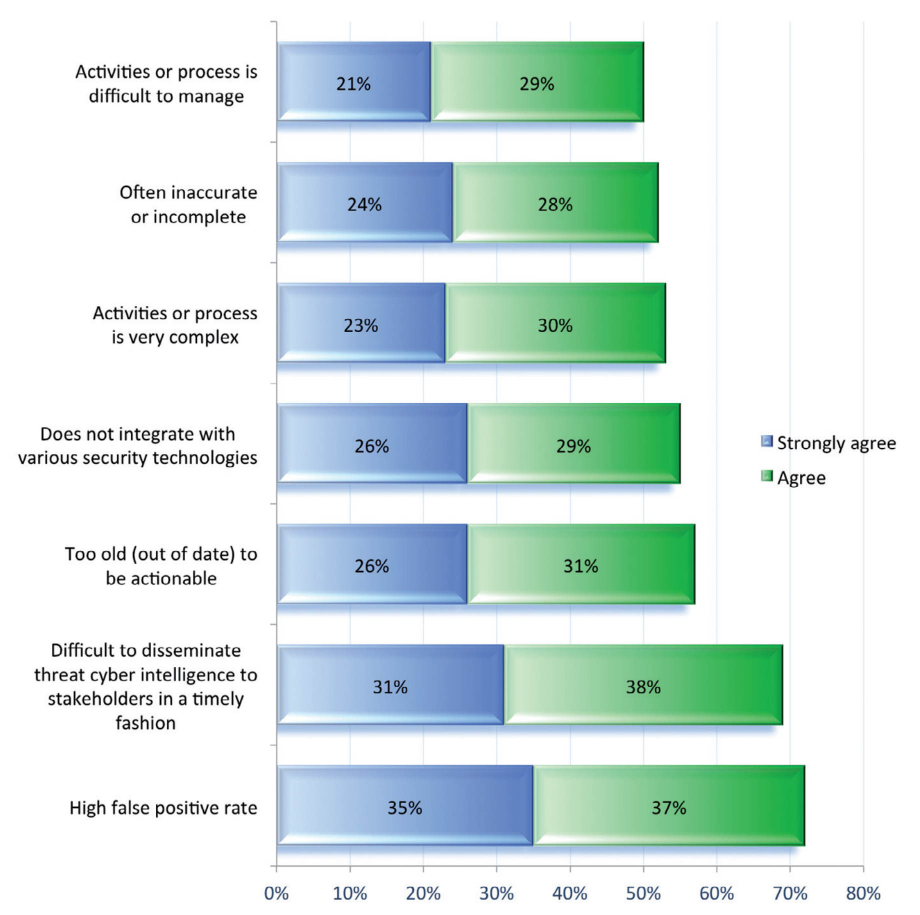
Intelligence-driven security

This is not a new message. Back in 2012, the Security for Business Innovations Council – which includes CISOs from the likes of ABN Amro, Coca Cola, eBay and JPMorgan Chase – said that in response to "advanced threats increasingly targeting corporations and governments", we need "a new approach called intelligence-driven information security ... The vision is to harness the power of information to prevent, detect and ultimately predict attacks".

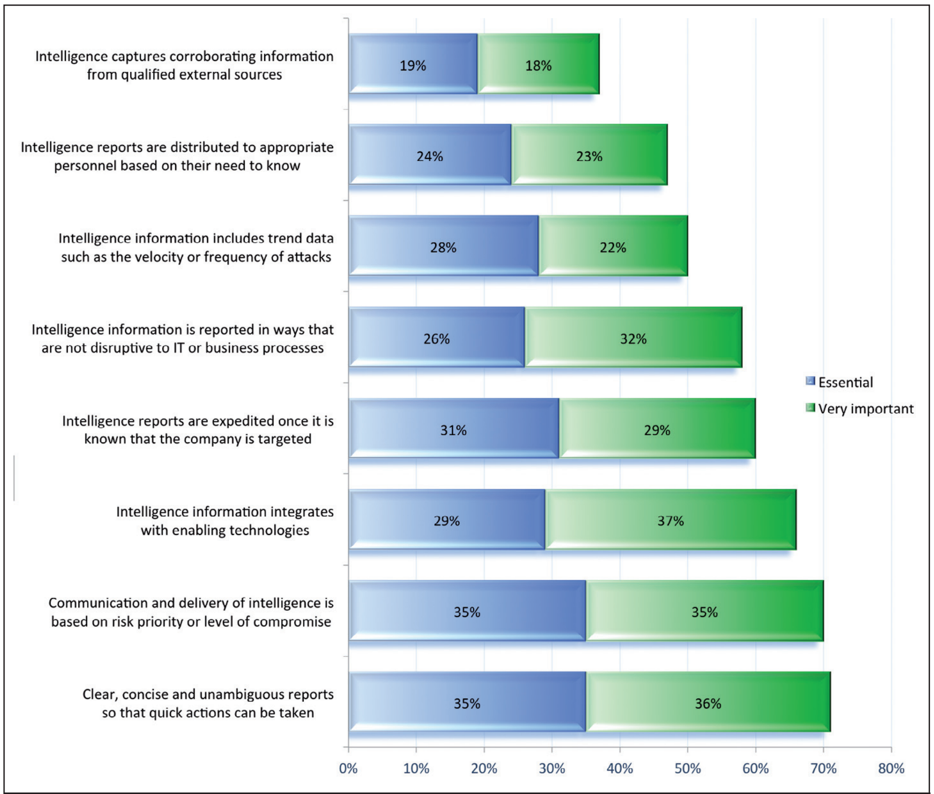
Likewise in July 2013, introducing his 'Live Threat Intelligence' study, Ponemon Institute chairman Dr Larry Ponemon said: "Readers of this report will come to understand that live threat intelligence must be an integral part of any security strategy."[1]

Earlier this year Andrew Beckett, head of consultancy at Airbus Defence & Space – Cyber Security (formerly Cassidian), said: "We firmly believe that intelligence and information sharing is one of five critical activities that you need to undertake if you are going to be relatively secure in a cyber context – the others being governance (leadership from the top and commitment to doing this properly), tools and techniques, standards and policies, and staff training."

But if the message has been repeated loud and clear, why did the UK Government need to step in in February and remind even the country's biggest, most critical infrastructure companies that we need more threat



Perceptions about problems with cyber threat intelligence. Source: Ponemon Institute.



Enabling security features that make threat intelligence reports more actionable and useful. Source: Ponemon Institute.

intelligence sharing? The answer is put succinctly by Paddy Francis, CTO at the cyber-security unit of Airbus Defence and Space: "There are too many people talking about information sharing and not enough doing it."

So what's going wrong?

Intelligence options

There's certainly no shortage of cyber-threat intelligence available, from both private and public sector sources.

"Increasingly, security intelligence and analytics is provided as a managed service, from the likes of IBM, HP, Verizon, Bluecoat, Orange, BT or Deutsche Telecom"

Commercially, established vendors such as Symantec, McAfee, Trend Micro, FireEye, Sophos, Kaspersky, IBM, Cisco and QinetiQ gather intelligence on new attacks all the time, and typically sell this information in the form of real-time feeds to their clients.

Other suppliers offer specific threat intelligence gathering, sharing and analysis products, like big data-based SIEM (security information and event management) or network intelligence tools – including Norse, Narus, HP ArcSight, AlienVault, McAfee, IBM-Q1 Labs and EMC-RSA.

Intelligence also comes packaged in wider security platforms, like Juniper, or built into security appliances, so included with the 'tin'. And increasingly, security intelligence and analytics is provided as a managed service, from the likes of IBM, HP, Verizon, Bluecoat, Orange, BT or Deutsche Telecom.

Managed services the way ahead

Clearly, the choice of vendors and products is wide but industry watchers point to two main trends: first, real-time 'live' threat intelligence is typically expensive and mainly the preserve of the biggest organisations; and second, managed services are providing a new and cheaper way for SMEs to get in on the act.

As Andy Kellett, principal security analyst at Ovum, says: "A lot of organisations will be looking at getting their security as a managed service – and with that, the security intelligence, the analytics, the reporting. So they are able to put those board-level reports together to say how effective they've been – levels of breaches, types of attacks, all that stuff that keeps them ahead of the game – even to the stage where things like SOC [security operations centres] as a Service will become more common within the enterprise."

Kellett adds: "I think managed security services is going to be a growing marketplace. I think more organisations will look at it as a resource they can call upon, not necessarily for everything they want to do in the security marketplace, but perhaps in areas where they themselves see a shortfall or are struggling to have their own resources in place, and I see security intelligence being part of that overall package."

"I would say that we have the basic intelligence but not the advanced security intelligence and that's what people are struggling with"

Larry Ponemon agrees this type of service could prove a lifeline for SMEs priced out of the current threat intelligence market. "We really haven't seen a lot of small companies improving their act," he says. "But there is a possible positive trend and that is these high-priced, high-falutin' systems that are designed for the million-dollar-plus budget – a lot of these vendors recognise the opportunity of selling to small companies and so they're coming up with cloud-based solutions where you can buy a seat rather than having to invest in the entire product."

Product problems

But there are issues with the commercial threat intelligence products available – including concerns among users that some of the software is not effective enough, or provides information that is out-of-date.

As Ponemon's Threat Intelligence survey damningly found: "Enterprises are using a wide range of technologies to gather threat intelligence, ranging from SIEM to IDS (intrusion detection systems) to IAM (identity and access management systems) and firewalls. However, on a scale of effectiveness, only 22% of respondents rate them between a seven and a ten, and 78% rate them between a one and a six."

The same survey adds that "57% say the intelligence currently available to their enterprises is often too stale to enable them to grasp and understand the strategies, motivations, tactics and location of attackers".

These findings are supported by Marc Vael, who as a board member of the global infosecurity professional organisation ISACA, represents CISOs.

"Most tools people that have to do with threat analysis are either based on the old logins – so they are reactive, every week or month or later even – or they are the ordinary type of access controls or password resets, that kind of stuff," he says. "I would say that we have the basic intelligence but not the advanced security intelligence and that's what people are struggling with."

Getting it for free

So what about the 'free' alternative? Why not access threat intelligence from the many public-sector sources that have sprung up, including academia, industry-focused and national CERTs (Computer Emergency Response Teams), and the Government's own CISP (Cyber Information Sharing Partnership), part of the UK's £860m National Cyber Security Strategy?

The driver behind all these schemes is this: given that everyone from nation-states to cyber-criminals and teenage hackers are targeting UK government organisations and general enterprises, then top-quality threat intelligence is too important to leave to chance and to the depth of your pockets.

Andy Kellett, Ovum: "A lot of organisations will be looking at getting their security as a managed service."

"The Government has been extremely proactive in developing CISP into an information-sharing collaboration tool which can be used by many organisations"

In particular, CISP, launched by the Government last March, has won plaudits. Cyber risk expert Chris Keeling, director of business continuity and crisis management consultancy Keystone Resilience, says: "The Government has been extremely proactive in developing CISP into an information-sharing collaboration tool which can be used by many organisations. The membership can get a very quick understanding of what is happening at the time and what the threats and vulnerabilities are."

CISP is designed to protect UK organisations by "facilitating the sharing of information on cyber threats between government and industry". Around 250 organisations are members (as of December 2013) across a range of industry sectors; and the Government is currently encouraging more companies to join, not just critical national infrastructure (CNI) ones.

CISP acts as a kind of private social-media portal where members log in, view and exchange information on threats and vulnerabilities in real time. It's driven by a central 'Fusion Cell' comprising people from GCHQ, the other security services, the National Crime Agency and industry partners.

CISP has an industry-based structure so automotive, financial services, aerospace companies and so on share with each other. Members are committed to putting in any information they have on attacks they have suffered, though they can choose to do so anonymously, to share just with the Fusion Cell, within their industry or with everyone participating.

Learning to share

Despite the obvious benefits of free threat intelligence sharing through CERTS, CISP and the like, there are problems with these programmes too – one main one being that people simply "don't share".

As Larry Ponemon says: "Conceptually it's a good idea but a lot of the CERTs, a lot of the programmes, they're running out of steam, they don't have a lot of resources. The problem is, they're looking for everyone to contribute, but the people who contribute might be a very small fraction of the community."

Ponemon has seen several cases where people fail to share threat intelligence within their own company – let alone outside it.

"There are silos even within companies," he says. "For example one datacentre in the UK might have intelligence but it doesn't necessarily have a vehicle for sharing that information with the datacentre in New York. So we see things like attacks that were identified in one part of the organisation months earlier, and successfully because that datacentre was able to protect itself. But instead of letting the world internally know, another part of the organisation gets zapped.

"The problem of intelligence sharing – that's actionable and at speed – that problem exists within companies and is probably a bigger problem than sharing across companies."

Keeling agrees: "There is this natural instinct not to share. In some organisations there is still the perception, be it real or not, of a blame culture – if something happens then obviously it's somebody's fault and somebody needs to pay the price for that, so people are naturally reticent about advertising it too widely. Also I think that in some cases they just don't realise that they should share information – they deal with it and then they don't share it."

The issue was even highlighted at a pan-European level last November when the EU's main cyber-security agency, ENISA, published a report called 'Detect, SHARE, Protect' (the 'SHARE' deliberately in capitals).

The report warned around 200 major CERTs across Europe – including 21 in the UK – that "the ever-increasing complexity of cyber-attacks requires more effective information sharing" but that those involved were showing a "lack of interest" in doing so.

Report editor Romain Bourgue said at the time the problem was that a few CERT teams were good at intelligence sharing, but gave up when others did not reciprocate: "You have a team that identify an issue that involves another team's constituency. They decide to share this information – which takes some time because you have to explain everything – and they don't get any feedback from the other team. If they do it once, twice, then the third time they will just not share this information because they don't get any feedback from them or it's only one-way."

Even if it is shared, Ponemon also questions how useful the data involved is. He says: "We do see some sharing in industry, through government organisations, but again a lot of what is shared is usually a little bit old, and not necessarily that actionable."

Getting personal

Even if organisations can instil a culture of sharing – and regardless of whether you buy your intelligence, get it for free or rent it through a managed service – there is a wider issue around threat intelligence sharing, which relates to the changing nature of cyber-attacks.

"Organisations need to focus not just on collecting and sharing threat intelligence, but also on their threat analysis and incident response –analysing attacks aimed specifically at their own organisation"

Take Waking Shark II, the high-profile cyber defence exercise conducted in the City of London on 12 Nov 2013, which tested how the UK banks would respond to a massive cyber-attack by a hostile nation state. Keeling was heavily involved in setting up this 'war game', which involved 20 banks and market infrastructure organisations. A key focus of the exercise and the subsequent report, which Keeling wrote, was the need for communications, "in particular information sharing among the firms via the CISP tool", which was heavily used but proved "difficult to manage".

Clearly, CISP and related programmes and products can play an important role in helping people share data on attacks where organisations are targeted together, like Waking Shark II; or where more than one organisation is targeted by the same cyber-attack with the same signature, like The Mask.

But Greg Day, vice president and CTO at supplier firm FireEye, points out that attacks are changing and becoming increasingly personalised. "There is a whole volume of public intelligence around what threats we are seeing on a day-to-day basis," he says. "But now we are seeing more and more personalised attacks and I think that then moves to a different kind of intelligence requirement. This is where the world is evolving – from cybercrime ('I want your bank details') which is very generic, to more targeted attacks which are after more high-value, commercial-value information."

In response, Day believes, organisations need to focus not just on collecting and sharing threat intelligence, but also on their threat analysis and incident response – not just sharing data to disrupt attacks across their industry sector, but analysing attacks aimed specifically at their own organisation.

And even though he is a member of the CISP steering committee, Day feels commercial threat analysis services are needed to top up what schemes like CISP provide. He explains: "We [FireEye] are obviously keen to support CISP because it's part of supporting UK plc. I think the likes of CISP can give some high-level guidance. But more and more I'm hearing organisations saying they measure the effectiveness of their security by their ability to respond to attacks – and that's not high-level guidance, that is the detail."

He adds: "If you talk to most organisations they will say 'we're breached every single day at some level or other'. So really what they want to understand is when there is a breach, what does it really mean? 'I got attacked and it was this bit of attack code' – but who's behind that, is that a hobbyist, is that a nation state, is that a group that's going to sell this to the Chinese'? More and more there is a demand for different levels of intelligence that say OK you've given me that high-level data that helped me recognise the scale and scope of the problem but now what I've got to do is understand the implications specifically to me."

Like Kellett at Ovum, Day suggests managed security services could play a role here: "We are seeing more and more organisations starting to outsource this area, either to having a managed security service or a managed SOC where getting the information is valuable but really what's important is 'what do I really do with that data'. I think that's where security vendors offer a commercial value in distilling down volumes of information into business-specific intelligence that is meaningful and actionable."

But this argument in turn is challenged by Vael at ISACA. Like others, he sees the importance of threat intelligence gathering, sharing and analysis, but feels it can best be done in-house.

"The higher-level trends analysis of transaction data – that is something that is really specific to organisations and you need to have specialists in the industry or even in the culture of the organisation to see what transactions they do, and if there is something going on that's not normal," he says. "It requires intelligence and knowledge on the inside to figure it out, that's what I've heard from our members. So you can't outsource that."

Conclusion

From Vince Cable to Ovum, from FireEye to ISACA, there is broad agreement that cyber threat intelligence is increasingly vital. But there the agreement ends.

Some pundits recommend sourcing intelligence from commercial suppliers. Others argue that's expensive and leaves out SMEs, while some users feel the products have some way to go before they consistently provide 'real-time actionable' intelligence.

Public sector alternatives, like the UK's CISP scheme and CERTs, win praise but may be undermined by the instinct for people not to share threat intelligence.

Managed security services are seen by many as the best way to cost-effectively understand new threats, who has attacked you and why. In particular, they could help SMEs who can't afford conventional intelligence sharing products – but then again, will SMEs switch on to the need for such activity?

"The ideal world for me would be if we had a mega-organisation for cyber that captures intelligence about potentially bad things, so that there's an advance warning capability"

Meanwhile, attacks are becoming more personalised, so there's a need to focus on individual threat analysis and incident response, rather than just gathering and sharing a mass of threat data. But whether that activity should be outsourced or kept in-house is another cause of debate.

In response to all these issues, one ideal solution has been put forward. Following Vince Cable's summit, James Stevenson, EMEA security director at vendor company Blue Coat, called for the UK to "build a nationwide, real-time repository of known malware, worms and threats" that would "allow businesses of all sizes to share information".

Likewise in the US, Ponemon told us: "The ideal world for me would be if we had a mega-organisation for cyber – but not a bureaucracy, not like another United Nations – that captures intelligence about potentially bad things, so that there's an advance warning capability. It doesn't operate necessarily for free but people participate because they're trying to protect their brands, their reputation and so it's a voluntary programme."

But is this a target or a pipedream? Just as everyone is talking about sharing but not enough people are doing it – so too everyone agrees threat intelligence sharing is important, but we are still inching towards finding the best way to do it.

About the author

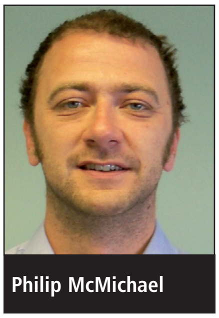
Tim Ring is a freelance tech journalist covering cyber-security and editor of IT Adviser Magazine.

Reference

1. 'Live Threat Intelligence Impact Report 2013'. Ponemon Institute and Norse, July 2013. Accessed Feb 2014. http://pages.ipvenger.com/PonemonImpactReport_LP.html.

The dangers of dead data

Philip McMichael, DiskShred


Philip McMichael

At end of service life every PC, laptop and server – as well as many laser printers and copiers – typically contain between one and 20 hard drives loaded with information. The chances are that some of that data is either sensitive or very sensitive, and in the wrong hands – eg, criminals or the hands of a competitor – this can spell trouble.

If even the smallest amount of that data is sensitive (eg, personally identifiable information, business intelligence or intellectual property) the whole drive must be treated as sensitive and the data on it disposed of safely and using a fully auditable process.

In today's datacentres and server rooms, the widespread use of virtual servers means that it is all but impossible to know what information is on a particular storage device. This means that it's impossible to know how sensitive that information is and so the only safe assumption is that it is highly sensitive and needs to be properly destroyed.