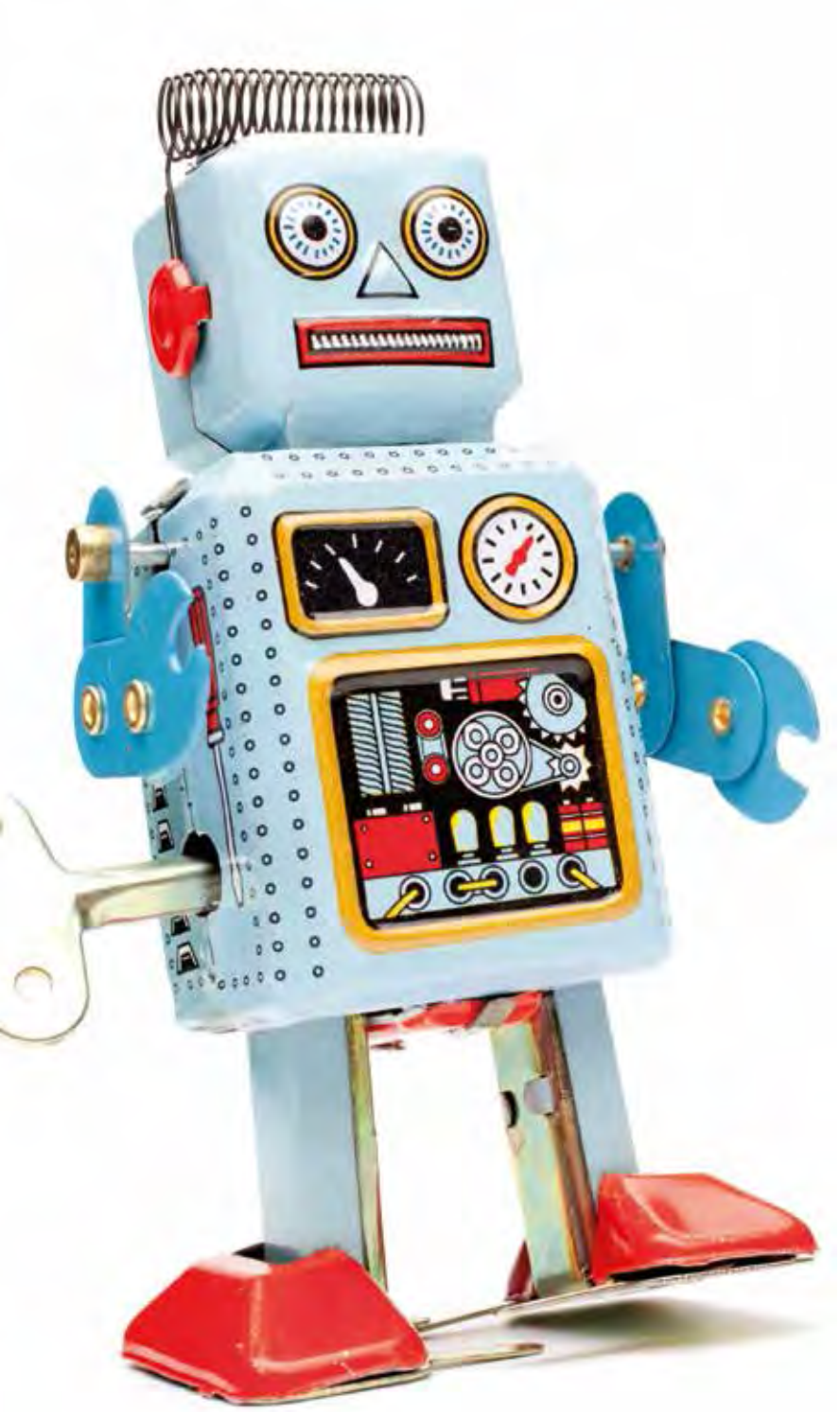
Cyber Threat Intelligence

Move to an intelligence-driven cybersecurity model



Stéphane Hurtaud
Partner
Governance Risk
& Compliance
Deloitte

Laurent De La Vaissière
Director
Governance Risk
& Compliance
Deloitte

Sébastien Besson
Governance Risk
& Compliance
Senior Consultant
Deloitte

The evolving cyber threat landscape

The business and technology innovations that organisations are adopting in their quest for growth, innovation and cost optimisation are resulting in increased levels of cyber risks. These innovations have likely introduced new vulnerabilities and complexities into the technology ecosystem. For example, the continued adoption of Web, mobile, cloud and social media technologies has undoubtedly increased opportunities for attackers. Similarly, the waves of outsourcing, offshoring and third party contracting driven by a desire to cut costs may have further diluted institutional control over IT systems and access points. These trends have resulted in the development of an increasingly boundary-less ecosystem within which organisations operate, and thus a much broader 'attack surface' for the threat actors to exploit.

Threat actors are increasingly deploying a wider array of attack methods to keep one-step ahead. For example, criminal gangs and nation states are combining infiltration techniques in their campaigns, increasingly leveraging malicious insiders. As reported in a Deloitte Touche Tohmatsu Limited (DTTL) survey[1] of global financial services executives, many financial services companies are struggling to achieve the level of cyber risk maturity required to counter the evolving threats. Although 75% of global financial services firms believed that their information security programme maturity is at level three or higher[2], only 40 percent of the respondents were very confident that their organisation's information assets were protected from an external attack. These figures apply to the larger, relatively sophisticated financial services companies. For mid-tier and small firms, the situation may be much worse, especially because resources are typically scarcer and attackers may see them as easier targets. In a similar vein, the Snowden incident has probably increased awareness of insider threats as well.

Being secure, vigilant, and resilient is a must

Organisations have traditionally focused their investments on becoming secure. However, this approach is no longer adequate in the face of the rapidly changing threat landscape. Put simply, organisations should consider building cyber risk management programmes to achieve three essential capabilities: the ability to be secure, vigilant and resilient.

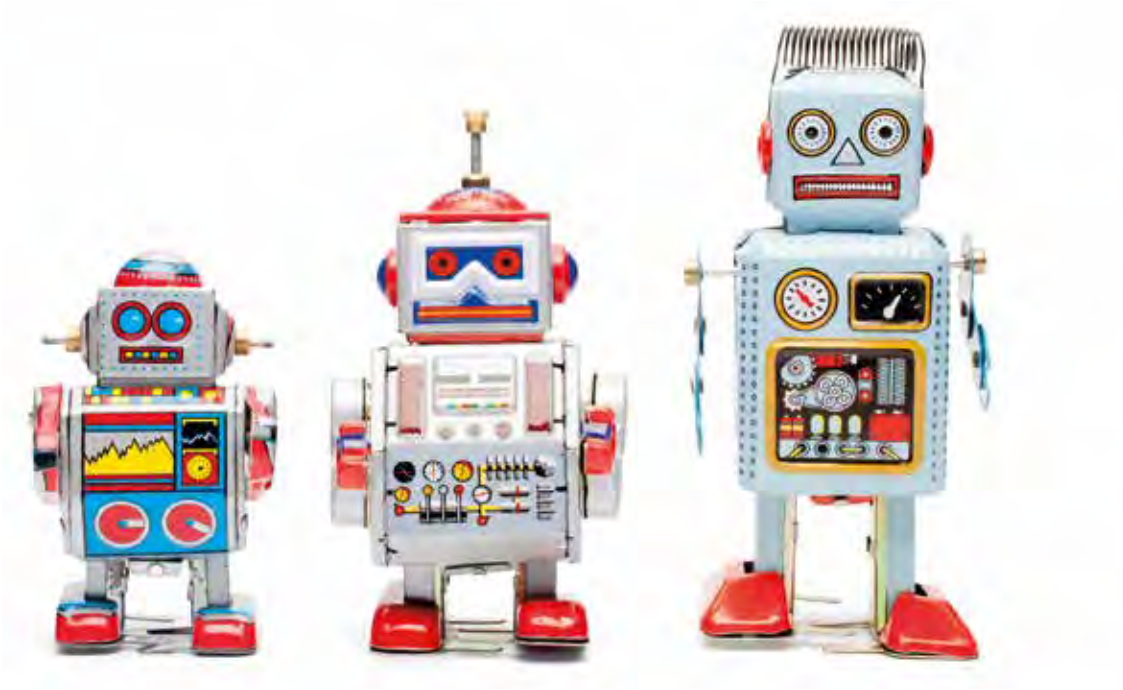
Enhancing security through a 'defence-in-depth' strategy: a good understanding of known threats and controls, industry standards and regulations can help organisations to secure their systems by designing and implementing preventive, risk-intelligent controls. Based on leading practices, organisations can build a 'defence-in-depth' approach to address known and emerging threats. This involves a number of mutually reinforcing security layers which provide redundancy and potentially slow down, if not prevent, the progression of attacks in progress.

Enhancing vigilance through effective early detection and signalling systems: early detection, through the enhancement of programmes to detect both the emerging threats and the attacker's moves, can be an essential step in containing and mitigating losses. Incident detection that incorporates sophisticated, adaptive, signalling and reporting systems can automate the correlation and analysis of large amounts of IT and business data, as well as various threat indicators, on a company-wide basis. Organisations' monitoring systems should work 24/7, with adequate support for efficient incident handling and remediation processes.

Enhancing resilience through simulated testing and crisis management processes: resilience may be more critical as destructive attack capabilities gain steam. Organisations have traditionally planned for resilience against physical attacks and natural disasters; cyber resilience can be treated in much the same way.

1 '2012 DTTL Global Financial Services Industry Security Study,' Deloitte Global Services Limited, September 2012

2 Survey defines 1-5 levels of maturity of organisation's information security programme. Level 3 – defined (set of defined and documented standard processes, some degree of improvement over time); level 4 – managed (process metrics, effective management control, adaption without loss of quality); level 5 – optimising (focus on continuous improvement, innovation)



Developing 'actionable' cyber threat intelligence

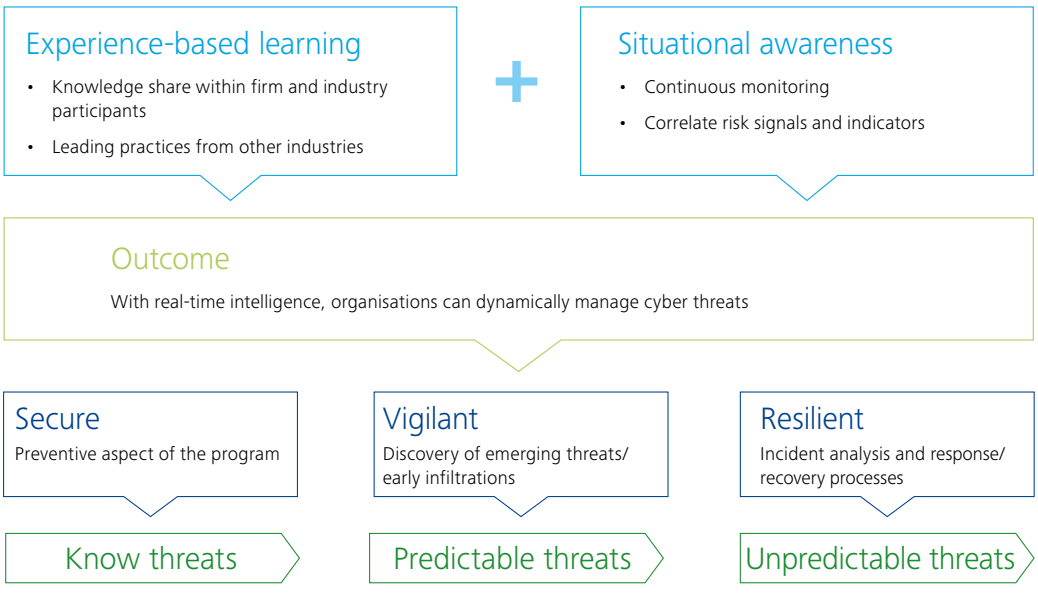
Executives recognise that becoming a learning organisation where intelligence drives actions is likely to be increasingly important for success across multiple dimensions. The realm of cybersecurity is no different, as real-time threat intelligence can play a crucial role in enabling security, vigilance and resilience.

"Availability of real-time intelligence can help organisations prevent and contain the impact of cyber attacks: a recent study[3] from the Ponemon Institute revealed that surveyed IT executives believed that less than 10 minutes of advance notification of a security breach would be sufficient time for them to disable the threat. Even with only 60 seconds' notification after the compromise, costs of security breaches may be reduced by an average of 40%".

By intelligence, we are not only referring to the collection of raw data about known threat indicators, as is provided by many vendors in the form of threat-intelligence feeds. Threat intelligence is also the ability to derive meaningful insights about adversaries from a wide range of sources, both internal and external, through automated means, and through direct human involvement.

To be actionable, threat data should be viewed in a context that is meaningful to the organisation. As a company develops greater maturity in its data gathering and processing capabilities, automation can be leveraged to better filter and highlight information that is directly relevant to important risk areas. In this way, threat intelligence becomes the foundation on which a firm builds its secure, vigilant and resilient capabilities.

So, how can organisations create that dynamism and move to an intelligence-driven cybersecurity model?



3 'Live Threat Intelligence Impact Report 2013,' Ponemon Institute (sponsored by Norse Corporation), July 2013

Experience-based learning

Just as cyber attackers play on their target's weak spots, so can organisations develop a sound understanding of the attackers and identify their Achilles' heels. Organisations can attempt to learn from past intrusions within the individual firm and at the industry level. Many companies can also borrow lessons from other industries, to implement new techniques, playbooks and controls. These lessons include understanding the nature of the attack, tactics and patterns, and containment strategies, and raise some questions that the organisation should consider to safeguard themselves from the onslaught of cyber attacks:

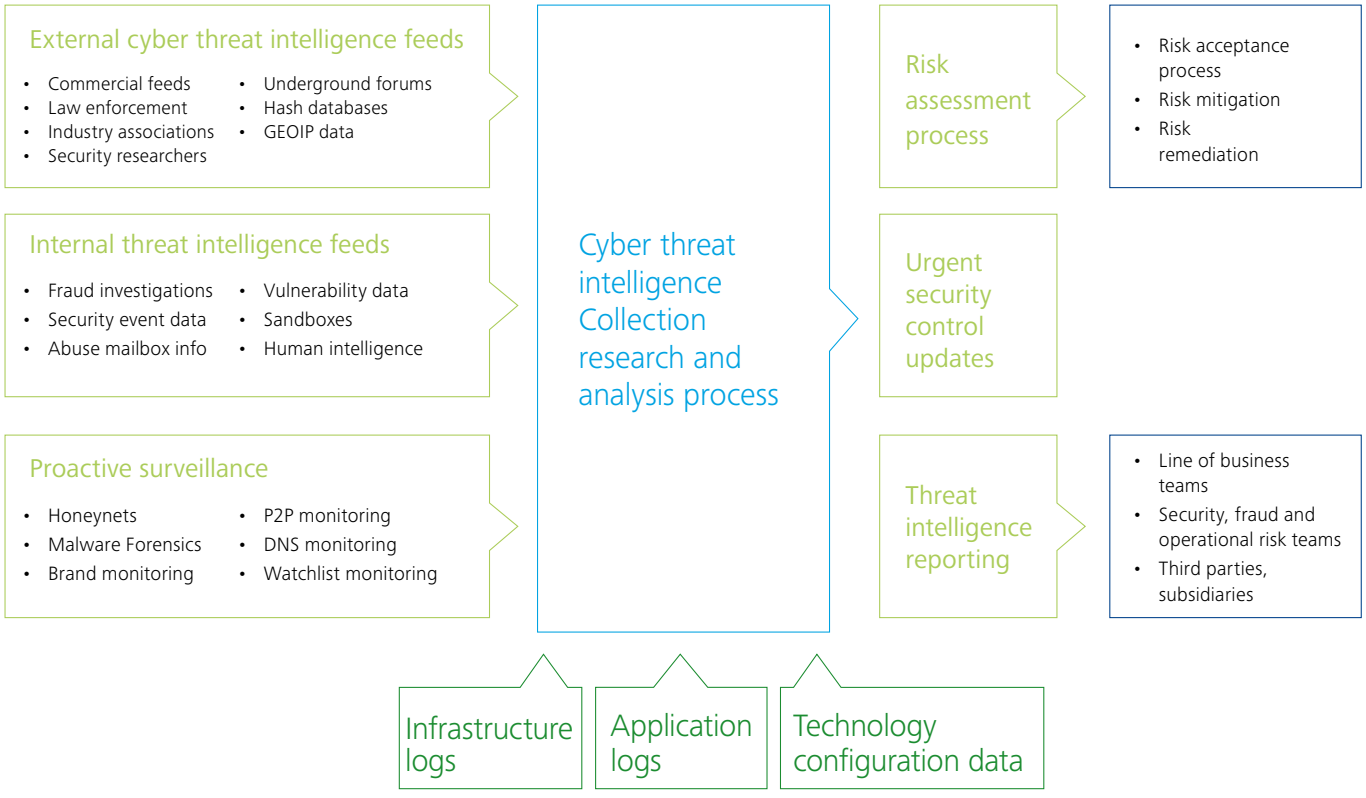
- Who are potential attackers and what are their motives?
- How do these cyber attackers manage such high attack success rates?
- Is it just the attackers' expertise or are the victims unwitting enablers? If yes, in what way, and how can that be fixed?
- What are some of the common challenges that attackers face while infiltrating organisations' systems?
- How are other organisations/industries dealing with such attacks?

Situational awareness

Organisations can consider supplementing experience-based learning with a continuous monitoring programme, focused on both external and internal threats. Continuous monitoring can help capture the risk signals and indicators across the ecosystem in order to develop a situational awareness of the threat environment. It assists organisations in identifying attack patterns and moving from being reactive to proactive in their defence and response mechanisms. Continuous monitoring also begins to address the speed-of-response issue that attackers are using against the financial services industry.

Cyber threat intelligence acquisition and analysis

The overall cyber threat intelligence acquisition and analysis process can be summarised as follows:



External intelligence feeds	Internal intelligence feeds
• Publications • Law enforcement sources • Industry associations • Security vendors • Underground forums • Hash databases • GEOIP data	• Fraud investigations • Security event data • Abuse mailbox information • Vulnerability data • Sandboxes • Human intelligence

Intelligence gathering

Gathering intelligence is a continuous activity. It involves choosing 'promontories' from which to scan the external environment and monitor the internal environment. Another way to think of them would be as 'channels' (akin to radio or television channels) through which you can monitor these environments. Promontories or channels include those that constitute external and internal cyber threat intelligence feeds.

While it pays to cast a wide net, there is always the factor of cost and the danger of sacrificing depth for breadth. So pick and choose your 'feeds' given your industry, needs and capabilities. Not every source will be useful to every organisation, and some will be more useful than others to a given organisation.

Proactive surveillance rounds out the intelligence gathering effort. Resources here include honeynets, malware forensics, brand monitoring, DNS monitoring and watch list monitoring.

A few of the specific technologies on which to focus threat research include the following:

Internet applications: online transactions, HR systems, wire systems, websites

Mobile computing: smartphones, mobile networks, text messaging services

Personal computers: operating systems, third-party applications, USB storage devices

Banking devices: ATMs, kiosks, RFID enabled smartcards

Telephony: voice response units, VoIP phones and PBXs, voicemail

Identity management and authentication: log-on, password, user code and other IAM technologies

Another potential source of intelligence would be the resources that potential adversaries use. Again, the goal should be to focus on devices and applications that expose the organisation's most valuable data, processes, activities and infrastructure to the most risk. Once a rich mix of intelligence is being acquired, efforts turn to analysis.

Intelligence analysis

The amount of data derived from broad-based intelligence gathering can be staggering. Therefore, analysis includes statistical techniques for parsing, normalising and correlating findings, as well as human review.

Six questions should drive this analysis:

1. How can we improve our visibility of the environment?
2. What new technologies do we need to watch for and monitor?
3. Do we have vulnerable technologies and data?
4. To what extent will our existing controls protect us?
5. Which industries are cyber criminals targeting and which techniques are they using and/or planning to use?
6. How can we identify actionable information?

This analysis should be conducted within a risk management process built around well-defined risk identification, prevention, detection, communication and mitigation activities. A cyber risk management process prioritises threats, analyses threats, detects a threat before, during or after actual occurrence, and specifies the proper response. The latter may consist of remediation, control updates, vendor or partner notification, or other actions. Analysis, such as failure modes and effects analysis, provides a feedback mechanism, such as lessons learned, to constantly improve the effectiveness of the analytics being performed.

Becoming a learning organisation

For many firms, becoming a learning organisation implies a need to develop an approach to address weaknesses in understanding their attackers' motives and methods. Learning from each experience and sharing information both within and outside the organisation will likely help many organisations deal with weaknesses in their ability to discover and recover from attacks.

Another potential source of intelligence would be the resources that potential adversaries use