Public

Swimming with Sharks

The existential threat of a cyber attack

September 2018

Synopsis

When, not if. That's the calculation you make when you are responsible for the integrity of complex, carrier-grade networks with more than 100Gbps of throughput. At commercial entities, government bodies or global service providers, nobody in the networking business is under any illusion. A cyber attack is a certainty, not a probability.

The scale of the threat is observable in the ever-increasing number of breaches and security incidents. It's there in the amount of spending on cyber security tools and the annual budgetary increases to protect vital assets. It's there when names like WannaCry and Wypr become part of the popular culture, and Stuxnet gets the documentary treatment from an Oscar-winning director[1].

More and more money, thought and talent is being directed to the prevention of a problem that, despite all that effort, isn't going away. So much so, that the World Economic Forum has identified 'massive cyber breach' as one of the top technological risks to continued global growth[2]. And, according to the Office of the Director of National Intelligence (DNI) in the US, cyber threats impose "costs on the United States and global economies" and presents risks for "nearly all information, communication networks, and systems." [3]

To operate in today's global economy is to swim in shark-infested waters. One sign of weakness, one drop of blood in the water, and you are at the centre of some potentially life-threatening attention. And like their marine counterparts, these sharks only need to be lucky once. Swim in these waters and you need to be lucky all the time, every time.

[1] Zero Days, directed by Alex Gibney, 2016
[2] World Economic Forum Global Risks Report 2017
[3] World Threat Assessment of the U.S. Intelligence Community. Director of National Intelligence, 2017

The cost of a breach

Recent corporate history provides us with plenty of examples of malicious cyber activity that has targeted both private and public bodies, and the consequences they have suffered. The most damaging attacks can take a number of forms:

- Distributed denial of services (DDoS) attacks that interfere with a firm's internet-based services rendering them unavailable.
- Destruction of property, including physical and virtual assets
- Theft of proprietary data, intellectual property, and sensitive financial and strategic information
- Business disruption, including for the purpose of collecting ransoms.

Generally, an attack will compromise or impair the confidentiality, availability and integrity of networks, communications systems, and devices, as well as the physical and/or virtual infrastructure that these systems control. Critically, they will also compromise the data stored, analysed and distributed by these systems.

Not surprisingly, therefore, businesses that experience this kind of attack can quickly lose the trust of the market, forfeit a good proportion of their reputation for sound management, and will see the overall value of the business drop.

In its most recent study[4], the Ponemon Institute has translated these abstract concepts into hard numbers. It shows that the total cost, the per-capita cost, and the average size of a data breach (calculated by the number of records that have been lost or stolen) have all seen a year-on-year increase.

Specifically:
- The average cost of a data breach per compromised record is US$148.
- The average total cost of a breach ranges from US$2.2 million for incidents with fewer than 10,000 compromised records to US$6.9 million for incidents with more than 50,000 compromised records.
- A mega breach (involving 1 million compromised records) can cost as much as $39.49 million.
- Businesses that use IoT devices extensively pay, on average, five dollars more per compromised record.
- It takes organisations an average of 196 days to detect a breach and 69 days to contain it.

Kaspersky Lab has also looked at the costs of a cyber attack[5]. Having questioned more than 6,000 employees at companies of various sizes and in various locations, it showed that between March 2017 and February 2018 the average cost of one incident to an enterprise is 24 per cent higher than in the 2016–2017 period, and 38 per cent higher than 2015–2016.

The exact financial damage caused by an attack will depend on the nature of the attack, and the victim's remedial capabilities and – as Ponemon noted – the number of data records held. But we can say that the total costs will encompass a full range of corporate activity, including: investigative forensics, regulatory penalties, PR and crisis communications, mandatory breach notifications, and customer protections. All of these may be relatively easy to calculate, but less quantifiable costs include: court settlements and fees, cyber security improvements, loss of revenues, cost of damaged equipment and lost data, cost of reputational damage, the increase cost of capital, loss of strategic information, and loss of IP.

Kaspersky Labs has broken down the average costs of an attack as follows:
- Emergency post-breach improvements to infrastructure and software: $193,000.
- Reputational damage, impact on credit ratings and consequent increase in insurance premiums: $180,000.
- Post-facto training for employees on security awareness: $137,000.

[4] The 2018 Cost of a Data Breach Study by the Ponemon Institute. Published by IBM, July 2018
[5] Kaspersky Lab: https://www.kaspersky.com/blog/economics-report-2018/22486/. Retrieved 1 August 2018

However, it is the work conducted by CGI, in conjunction with Oxford Economics, that shows the most eye-watering numbers. Following a severe breach, CGI calculates that the share price will fall by an average of 1.8 per cent and will never recover.

In extreme cases, breaches have wiped as much as 15 per cent off company valuations. To put that in context, at a typical FTSE 100 firm this kind of damage equates to a permanent loss of market capitalisation of £120 million[6].

Who are the sharks

Having calculated how much damage a cyber attack can do, it is essential to understand who is responsible for them. Fortunately, using a number of expert resources, the Council of Economic Advisors in the US has produced a detailed analysis of cyber threats facing individual companies and the US economy as a whole (and thus, by extension, the global economy).

It has divided the potential perpetrators of cyber attacks into six broad categories:

1. **State actors:** That Putin's Russia is a key source of cyber threats should come as a surprise to no one. However, it is China and its thirst for information that may be the biggest state actor in the corporate sphere. The DNI also considers as threats both Iran and North Korea, the latter of which was responsible for the WannaCry malware attack that cost the global economy billions of dollars. Nation-states are well funded, often sophisticated and driven by a combination of political, economic, technical, or military factors. Nation-states also engage in industrial espionage, ransom attacks and theft of funds.

2. **Corporate competitors:** Industrial espionage has been going on for as long as industry has existed. Inevitably, as commerce gets more sophisticated, so does the spying. All firms face the fact that their proprietary IP, including financial, strategic, and workforce-related information, is valuable to competitors, some of whom may seek illicit access to it. It's also worth noting that many of these corporate threats are backed by the state.

3. **Organized criminal groups:** It was inevitable that offline organized crime would move into cybercrime once it became sufficiently lucrative and more cost effective than the shoe-leather and staffing required for more traditional 'business' models. These organizations undertake targeted attacks and are motivated purely by profit. Personally identifiable information (PII) is usually the target: a valuable asset that can be sold on the dark web to the highest bidder(s), be used to collect a ransom from public and private bodies, or both. Paying the ransom is no guarantee that the data will not be sold anyway. Attribution of cyber events is always difficult, but Verizon's Data Breach Investigations Report notes that 51 per cent of threat actors involved organised criminal groups.

4. **Hacktivists:** Usually driven by a political agenda, hacktivists tend to be private individuals or groups who carry out high-profile, headline-grabbing attacks to gain attention for their cause, to disrupt or damage their opponents, or to distribute propaganda. Anonymous, WikiLeaks, 4Chan and LulzSec can all be classed as hacktivists, as could individuals like Chelsea Manning.

5. **Company insiders:** If you have a seriously disgruntled employee or ex-employee looking for revenge or financial gain, you could be open to an inside job. Should these individuals work with external actors, the risk is heightened since the two-prong approach makes it easier for outsiders to bypass robust defences.

6. **Opportunists:** Deemed by some as asocial amateurs looking for notoriety, opportunists usually attack organisations using codes and techniques that are already widely available. They are therefore usually the least sophisticated adversary, and will be successful more by luck than judgment.

[6] The Cyber-Value Connection, revealing the link between cyber vulnerability and company value. CGI, 2017.
[7]The Cost of Malicious Cyber Activity to the U.S. Economy, The Council of Economic Advisers, February 2018

Choppy Waters

These costs and the threat actors continue to evolve. But the constant in this sector is that maintaining a carrier-grade network is about ensuring “five nines” high availability standards as well as very fast fault recovery. Redundancy of less than 50 milliseconds on high-rate networks that can process tens of hundreds of gigabits a second is also a must.

This has always been a technical and operational challenge. But as we have seen from the Kaspersky and Ponemon research, the more data points on a network, the more costly an attack will be. Graphs showing not just global threats, but global data rates, global subscribers, internet users, and network users will all show a curve with a dramatic upward incline. This is the primary source of the current problem: the sheer volume, value and velocity of data at rest and data in motion is degrees of magnitude greater than has ever been seen before.

Consider the following:
1. The phone in your pocket has more computational power than was available to NASA when it sent the first men to the moon
2. When Windows 95 was launched in the mid 1990s, computers were capable of approximately four million operations a second but are now running ten trillion operations a second
3. Just one of the latest computer chips to go into production has the same power as the supercomputers that headed the TOP500 ten years ago.

It is almost inevitable, therefore, that the increase in size, frequency and damage caused by cyber attacks would mirror this growth. What’s more, technological advances including machine learning (ML), the Internet of Things (IoT), IT/OT convergence, smart and distributed energy grids, and the ongoing proliferation of mobile and micro-devices, will contribute even greater number of endpoints, ‘things’ and devices that cannot protect themselves to the network. All will generate even more data and infrastructure to be protected.

Technological advances are also being used by the other side. Although plenty of cyber professionals are using AI and ML software to learn from past events to predict and identify future threats, so are cyber criminals. So although AI is used by approximately 87 per cent of US cyber-security professionals, 91 per cent are concerned that threat actors will use AI to create even more sophisticated attacks[8].

Of course, attack vectors continue to evolve: according to Akamai, summer 2018 saw a new threat vector emerge in the form of Memcached reflection, as well as a new record DDoS attack of 1.35 Tbps. Botnets and other forms of distribution make DDoS attacks almost ubiquitous: overall the number of DDoS attacks increased by 16 per cent, as did attacks on the infrastructure layer (layers 3 & 4), while application-layer attacks increased by 38 per cent. DDoS attacks are also used to mask other under-the radar threats. Akamai also reported that the Dutch National High Tech Crime Unit and the UK National Crime Agency teamed up in “Operation Power Off” to take down a commoditised DDoS platform[9].

Unfortunately, the application of cyber defences has not always kept pace with the growth of the estate that must be protected or the capabilities of those inflicting the attacks. As we discuss below, this applies to technological remedies: carrier grade networks require carrier class security, and this is not always in place. But it is also worth considering the operational picture. The damage of a single attack often spreads out beyond the initial target to hit businesses, partners and customers that are economically linked to the original subject. One attack can therefore damage a broader ecosystem and ripple throughout the entire economy. Equally, a business can be made vulnerable through its connections to other organisations. This is one of the reasons that reputational damage can be so costly: it’s not just individual consumers who will feel the impact, but large corporate and governmental customers.

[8] The 2018 Cost of a Data Breach Study by the Ponemon Institute. Published by IBM, July 2018
[9] Kaspersky Lab: https://www.kaspersky.com/blog/economics-report-2018/22486/. Retrieved 1 August 2018

What's more, businesses in a common field often share common cyber vulnerabilities, which means that if one firm is hit, others are at immediate risk. The whole problem is compounded by a scarcity of data about individual attack vectors, as well as a lack of information sharing between organisations. This relatively isolationist approach hinders cybersecurity efforts in both prevention and detection. Incidentally, it is also a hurdle to the development of an effective and efficient cyber-insurance market.

Finally, as with all security measures, there is a balance to be had between protection and usability. For example, maintaining an air gap can protect individual computers or even an individual network, but it comes with a calculated compromise to the functionality of that device. In any case, it is obviously not a viable solution for a network-centric business and its customers. In addition, the pressure to secure and protect the network and its data has to be offset against considerations around net neutrality, freedom of the internet and data privacy. Discard all these issues, and protection becomes easier; but again, strategic business objectives may be abandoned.

Inadequate defences

The underlying principles of cyber security are rapid identification and rapid containment. These threats are not always bombs that flatten a building on impact. They are often slow release poisons that infect and re-infect until they are stopped. So organisations need to:

- Understand the number and volume of threats that they face
- Understand the threat density of their network
- Understand the 'grade' of the threats on the network

To do that, they need the right tools that can provide protection at multiple layers. This includes, but is not limited to technology that can:

- Provide visibility of the entire network in order to detect and then prevent cyber attacks or data breaches.
- Conduct Network Performance Monitoring & Diagnostics (NPDM) to analyse IP traffic flows, engineer traffic, arrange billing and monitor security and generate meta data on traffic flow.
- Detect threats and breaches using signature matching against known threats.

Currently, organisations are using a mixture of existing commercial and proprietary solutions. However, the argument for these solutions was far more convincing ten years ago than it is today. Simply put, the rate and capacity of networking platforms has increased exponentially in the intervening years, while latency has decreased.

While networks generate millions of events each second for analysis, many existing analysis tools are designed to process up to 20,000 events per second. Similarly, existing tools that generate meta-data for monitoring flow cannot cope with increasing data rates, and are usually not viable at rates above 20-30Gbps. The same is true when it comes to signature matching. Security analysts need to inspect every packet travelling through the network, but again most currently available intrusion detection systems run at 1Gbps or lower. What's more, recording all of the data packets from a session for off-line analysis can prove to be prohibitively expensive, while extracting a single session from all the data recorded can be very slow and processor intensive.

Solutions designed for a smaller data set and a slower rate will struggle to scale and be fit for purpose in the current high-rate environment. It will also typically have a longer refresh cycle so that it fails to keep up with new threat vectors as they emerge. To get round this fundamental problem of not being able to visualize all network traffic, identify potential anomalies or monitor suspect activity, firms rely on sampling or pre-selecting the specific activity they choose to look for.

But this too is no longer appropriate. Take sampling for example: an operator of a carrier network looks at one in 8,000 internet sessions, and takes any remedial action based on that one in 8,000 sample. When DDoS attacks first emerged, this level of sampling could identify and contain a brewing attack. However, attackers have changed their MO, favouring low-rate denial of service attacks or single-flow threats such as phishing, data exfiltration, or individual spiral attacks. In these cases, an attacker can use one session to steal all your customers' credit card data. If your one in 8,000 sample is looking at another session then your customer data will be gone before you spot it.

Firms relying on an in-house solution also face the problem of staffing: to counter the difficulties that these tools experience, firms need vast and agile development teams that can look at every single flow, detect each brewing attack, and respond to rapidly evolving threat vectors. The in-house option has become an ineffective cost sink that gives a false sense of security when it comes to threat and risk mitigation. To go back to our shark analogy: it's relying on a home-made cage made of raw steak.

The shark proof cage

The threat is multi-faceted and so is the solution. Operators of carrier-grade networks require a multi-layered approach based on a number of carrier-grade tools that are designed to operate in 100Gbps-rate networks. In particular, organisations should look for:

1. Integrated network visibility software for cyber security and performance management that can:

- Ingest and analyse data at a national network scale, with tens of millions of unique endpoints, and millions of events per second.
- Ingest data from multiple sources to enhance and accelerate network data analysis and workflow.
- Scale across infrastructure based on multiple servers.
- Provide a cache that allows sub-second latency for queries on stored data.
- Group IP addresses into sets for rapid filtering and metrics.

2. Tools to monitor networks in real-time and scrutinise every packet for total network visibility at rates up to 100Gbps, including:

- Analysis of flow records for anomalies, zero-day threats and other advanced persistent threats.
- Incident response in the form of historical analysis as well as NPMD.
- Diagnosis of slow network performance, bandwidth hogs and bandwidth use.
- Detection of unauthorized traffic and accurate analysis of user and network behaviour.

3. Event-driven intrusion detection system and recorder that can:

- Integrate with Security Incident Event Management (SIEM) to quickly identify true threats and eliminate false positives.
- Generate IDS alerts and can record an individual packet or entire session.
- Provide intelligent record appliances for incident response and forensics at 40Gbps.
- Trigger smart packet capture on threat detection and offer rapid session search and reporting.

Summary

Carrier networks need carrier grade security. They require a system that can take on and analyse millions of pieces of data from millions of endpoints across an organisation and identify areas of concern in real time. Organisations of all kinds that operate without the necessary specialist technology infrastructure will see their investors, shareholder and customers making do or swimming for safety.

But cyber security is also a common good. Sloppy cyber security imposes costs and negative impacts in all kinds of ways on all kinds of organisations as well as private citizens. Underinvestment in cyber security by both private and public bodies leaves us all with a level of protection that is significantly below what we require as a society.

Organisations that don't invest will be left behind as shark food. The trick is to make sure that individual citizens and civil society as a whole is not left there with them.

Headquarters
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
t. +44 (0)1258 480880
f. +44 (0)1258 486598
e. sales@telesoft-technologies.com

Americas
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
e. salesusa@telesoft-technologies.com

Asia
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301, India
t. +91 120 612 7725
e. salesindia@telesoft-technologies.com

telesoft-technologies.com