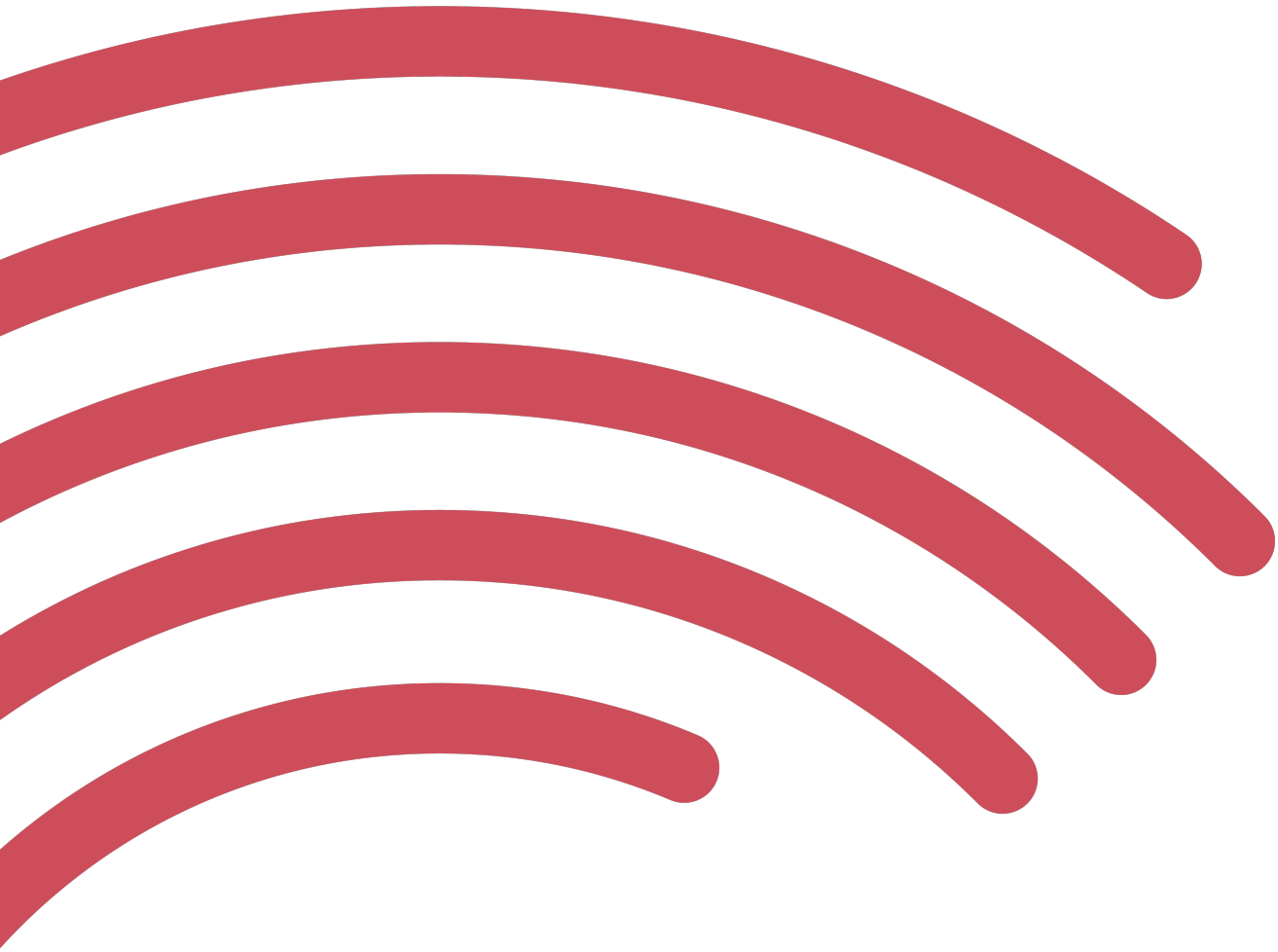
CYJAX

Digital Intelligence
Securing the Future



4R and 4D

CLIENT CONFIDENTIAL

4 Rs of Analysis and the 4 Ds of Threat Modelling

Introduction

Applying an enterprise-level risk model to a small or medium sized-enterprise (SME) can be a frustrating undertaking. Nowhere is this more apparent than in the often-missing underlying documentation, such as an asset inventory, configuration database, service catalogues, and current network mapping. Realising, too, that to provide effective insights and ultimately be successful, a Cyber Threat Intelligence (CTI) program has further requirements still, this process can seem an almost impossible task.

One such requirement is the explicit identification and approval of "Intelligence Requirements" prior to any CTI program being launched. What does this program need to provide? What are the restrictions and limitation in scope? And who's responsible for making approvals? Answering these questions is vital for both in-house programs and 'CTI-as-a-service.' This paper will provide the starting point for the construction of fact-based intelligence requirements for a robust CTI program.

To understand the SME's risk, there needs to be agreement on the relevant threat models or scenarios that could result in a security event for that organisation. These threat models must be applied to avoid a situation in which "everything" is deemed a top priority, and where "everything" needs to be detected and proactively avoided. This will lead to an overwhelming amount of work and program failure. Even government agencies with black budget funding in the billions of dollars will miss some impactful events. A conscious effort is required to facilitate the identification of the most likely to occur scenarios with a keen understanding of the impact on the organisation should any of these occur.

It is fair to say that most SMEs have little experience of enterprise risk strategy and will, therefore, be unable to communicate at the esoteric and sophisticated level associated with enterprise risk management teams. This is due to the presence of SME legacy systems in the IT environment, where accurate metrics may be elusive at best and complete fiction at worst. Most SMEs will be less organisationally complex than enterprises. A scaled-down and simplified approach is, therefore, highly desirable. Threat models or scenarios are the easiest way of building an SME CTI program, founded firmly in each organisation's business reality.

You may be familiar with the qualitative risk equation: consequence multiplied by likelihood. Consider a similar approach here. We will assess the consequence of the 4 R's: Revenue, Reputation, Regulation, and Resiliency. And we will compare them against the likelihood of the 4 D's: Disruption, Destruction, Degradation, Deception.

What cybersecurity scenarios could impact company revenue?

Analysis by Revenue

The relationship between the accounting department and IT is an interesting one. The information needed for threat modelling against revenue generation should be informed by several things. Specifically, data from the accounting department wherein different lines of the business's revenue are broken down from the most to least profitable. This analysis can be taken one step further by including customers that are responsible for generating the most revenue for a particular business line.

Some thought needs to be given to the impact that an attack on IT systems will have on revenue generation, such as customer billing, trading, or production line activities. The higher the revenue from a specific area of the business, the greater priority should be given to determining intelligence requirements related to disruption, destruction, degradation or deception activities that result in the organisation losing revenue.

Example Threat Models:

- Revenue Disruptive threat model: Ransomware attack.
- Revenue Destructive threat model: Regulatory penalties, etc.
- Revenue Degrading threat model: Sudden increase in competition or cost of goods.
- Revenue Deceptive threat model: Business Email Compromise (BEC).

By applying the 4 D's to sources of revenue, the intelligence requirements for the CTI program can be quickly identified.

Example Intelligence Requirements:

- Indicators of compromise attributed to threat actors with a history of attacking the organisation's industry vertical.
- Monitoring of legal precedents and court decisions which may impact claims against the organisation.
- Monitoring of supply chain, as it relates to revenue generation.
- Incidents of BEC attacks, and active campaigns on the organisation's industry vertical and supply chain partners.

The CTI program must demonstrate the integral role that IT services play in revenue generation. Frequently, there will be dependencies on services provided solely by IT – such as DHCP, DNS, internet connection(s), Wi-Fi, and on-site or hosted infrastructure. The extent to which these foundational services can impact revenue generation, and the relevant threat model, need to be documented. The CTI program cannot develop accurate intelligence requirements if there are unknown dependencies.

If the primary revenue-generating function for an organisation is an eCommerce website which receives customer orders, the application of the 4 D's to the website will provide a clear picture of the most likely events that may impact the website's ability to function. These threat models could range from an insider threat to overt attacks such as DDoS, and even covert attacks such as Magecart JavaScript injection designed to steal credit card information. The CTI program would establish intelligence requirements to proactively monitor for incidents such as this.

Analysis by Reputation

The marketing, public relations or sales department should be engaged to assist the CTI program in determining the organisation's reputation in the industry, and what impact a security event may have on that reputation. In most marketplaces and industry verticals an organisation's reputation is related to the market share it has obtained. Major security events may have a profound effect on the willingness of consumers to continue doing business with the organisation. Other likely effects of a major security event include difficulty in recruitment, existing employees moving on, and key suppliers reevaluating their relationship with the organisation. Headlines regarding TSB's failed IT projects and disruption by malicious actors, are perfect examples of these security events.[1]

Example Threat Models:

- Reputation Disruption: Poor change management practices.
- Reputation Destruction: Irretrievable loss of customer data.
- Reputation Degradation: Competitive displacement campaigns.
- Reputation Deception: Public scandal involving corporate wrongdoing.

Example Intelligence Requirements:

- Monitoring of social media related to customer satisfaction and sentiment
- Monitoring of disaster recovery and business continuity posture of organisation
- Monitoring of competition marketing activities
- Monitoring of media and trade publications for information of concern

Another consideration for reputation analysis is for the CTI program to understand what the contractual obligations and agreements are between the customer, supplier or third party. Many contract agreements have penalties associated with violation of partnership terms, which may translate into a direct monetary penalty – as discussed under analysis by revenue.

There are any number of additional threat models to apply to Analysis by Reputation. These may include Website defacements, DDOS on customer-facing portals, and social media firestorms. The CTI program will need to understand the impact of these threat models on supporting systems. A customer-facing reputation-disrupting event, for instance, system outage, may degrade or render call centre related activities unavailable to customers – a knock-on effect. In a highly competitive market, the reputation of the organization is a key part to continued success, and any reputational attack may have a longer-term impact on growth and revenue. Threat models must anticipate the reputational damage of, for example, an e-commerce site with no internet connection, or an inbound call centre without VoIP services.

Analysis by Regulation

The councils office, CFO, compliance team, or organisation's law firm is likely to have information about precisely what regulations are applicable to the organisation's business operations. Notwithstanding the previous revenue-based and reputation-based analyses, certain systems may have life safety or critical infrastructure designations. These require minimum cybersecurity standards and/or public breach disclosure. Other systems, such as those under PCI DSS, GDPR, or HIPPA have security requirements with potentially devastating fines for violation. In heavily regulated industries the FCA (UK), ICO (UK), FCC (USA), EPA (USA), and multiple other US government agencies, could bring an action against the firm depending on the nature of the business system outage or statutory violation. Regulatory action is not always done privately and, as such, may impact reputation as much as it does revenue.

Example Threat Models:

- Regulation Disruption: change in the PCI DSS audit requirements for your organisation.
- Regulation Destruction: new regulation, such as GDPR, which could potentially curtail operations like Business to Customer emails.
- Regulation Degradation: new regulation or compliance requirement which may increase costs.
- Regulation Deception: fraudulent attestation of regulatory compliance which is not supported by evidence.

Example Intelligence Requirements:

- Monitoring of any change notifications related to audit standards.
- Monitoring of new legislation, and its potential impact to the organisation.
- Monitoring of industry trade association's costs of compliance.
- Monitoring of audit reports ensuring that they are fact-based and supported with evidence of compliance.

Some organisations may see a CTI program as intrusive in terms of Regulation analysis. This may stem from many of the intelligence requirements relating to documents and activity which is far outside the realm of cyber threat. While this is certainly the case, in order to provide a comprehensive view of the organisation, the CTI program's ability to monitor information sources, conduct analysis and send the information to the right team members has tremendous proactive value. Compliance with regulations is rarely optional, so from a threat model perspective, any 'D' threat model impacting compliance could be a serious matter.

Analysis by Resiliency

This is generally a technical domain of the IT department, which should have an idea of systems' weaknesses and points of strength. If empirical data is needed, an examination of the ticketing system by department may provide insight into systems with questionable reliability. A review of any security incidents may also prove insightful for the CTI team.

An organisation's current infrastructure is likely to be heavily dependent on internet connectivity. Those systems that are not dependent on internet connectivity, or are not customer-facing, have an inherent resilience against a disruptive cyber event. Loss of external internet connectivity, for instance, may allow on-premise production or in-house applications to operate without impediment.

Understanding systems which can run when external connectivity is degraded or unavailable will inform the overall focus of the CTI intelligence requirements. The main input for this analysis is informed by network architecture and existing network segmentation. On-premises solutions, isolated from internet connectivity, should be a lower priority: these are generally only accessible inside the corporate network or available over a dedicated point-to-point connection.

System architecture has a significant effect on the setting of intelligence requirements and prioritisation of intelligence products. A remote code execution (RCE) vulnerability, under active exploitation by a threat actor against a system that has no exposure to the internet, may not be as concerning as one that is exposed on your public-facing IP.

Open-source and some proprietary environments do present a slightly larger CTI challenge. Some detailed knowledge of the sub-system environment will be required to define the intelligence requirements. WordPress and Drupal are two of the world's most popular Content Management Systems (CMS), and many organisations use them both internally and externally to deliver services. These two CMS products are made up of myriad sub-systems, such as MySQL & Apache, as well as several plugin components to assist in website functionality – such as a contact us form.

The CTI program must understand that a vulnerability under exploit for Apache, for example, has the potential to impact the CMS environment. Intelligence requirements should be designed to address solutions used within the environment and its related sub-systems.

Apache Struts (CVE-2017-5638) was the vulnerability that led to the massive and well-publicised data breach at Equifax. The question of course is: could a CTI program have identified and warned Equifax in time for remediation to have taken place? The answer is, 'possibly'. It would have required an exceptional CTI program, backed by a powerful executive to command the company's resources to rapidly execute remediation.

Equifax's data breach was unprecedented. It included sensitive personal data of 148 million Americans. The data breached included names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also breached. Let's look at a timeline of the most interesting issues – It's important to keep in mind that CVE-2017-5638 was not an easy patch to apply

- On 10 March 2017, the National Vulnerability Database (NVD) issued a CVS:10/10 (the highest possible rating) warning: "The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1… allows remote attackers to execute arbitrary commands."[2]

- Prior to that warning the first widely available public blog concerning the remote code execution (RCE) vulnerability in Apache was by Cisco Talos on 8 March 2017.[3] "Forensics analyzed after the fact revealed that the initial Equifax data breach date was March 10, 2017: that was when the web portal was first breached via the Struts vulnerability."[4]

In this case, even if the CTI program's intelligence requirements had included "monitoring CVE's with a rating of 7+ vulnerabilities for externally exposed system components and sub-components", it is unlikely that the Equifax IT department would have been able to patch and update the vulnerable systems within 48 hours. The likely recommendation of a particularly thorough CTI program, to temporarily remove the vulnerable systems from the internet, would have been met with stiff resistance from executives.

The timeline of the Equifax data breach presented by the Electronic Privacy Information Center (EPIC) reveals significant shortfalls in vulnerability management on the part of Equifax:

- 7 March 2017- The Apache Software Foundation reported the vulnerability Apache Struts CVE-2017-5638 and released a patch.
- 8 March 2017- Department of Homeland Security (US-CERT) contacted Equifax, Experian, and TransUnion to notify them of Apache Struts CVE-2017-5638.
- 15 March 2017- Equifax's information security department ran scans meant to identify systems that were vulnerable to the Apache Struts issue, but the scans did not identify the vulnerability.
- 13 May 2017- Malicious actors began to access personal identifying information.
- 29 July 2017- Equifax discovered "suspicious network traffic" associated with its consumer dispute website after renewing a certificate which had lapsed some nine months prior to these events. Equifax information security department applied the Apache patch. [5]

Even though it appears malicious actors – later attributed to China's People's Liberation Army (PLA)[6]– had gained a foothold on 10 March, they did not attempt data exfiltration until 13 May. Why did it take two and a half months to detect suspicious activity?

CTI could have made a difference. If the CTI program had "monitoring encryption certificate status for internal security tools" as an intelligence requirement it is highly likely that the exfiltration attempts on 13 May 2017 would have been detected and thwarted. The breach of 148 million Americans' sensitive data may never have happened.

Some organisations will have an inherent level of resilience due to digital transformation. In the case of SaaS solutions from third-party providers or applications moved to public data clouds, these systems may have high availability. Furthermore, some of the security controls may be outside the responsibility of the organisation to maintain, due to a shared responsibility model. It is not uncommon, however, for a CTI program to monitor these critical third-party providers for security events – such as a publicly disclosed data breach and recommend appropriate action jointly.

Example Threat Models:

- Resilience Disruption: changes, upgrades and business projects may change the resilience significantly – Single Sign-On technology may be a single point of failure.
- Resilience Destruction: system growth impacting network capacity and size of the database may impact the ability of the organisation to return to normal operation.
- Resilience Degradation: lack of lifecycle management and requirements for enhanced security controls may degrade the resilience of the system.
- Resilience Deception: untested or undocumented Disaster Recovery or Business Continuity may lead to incorrect assumptions concerning system resilience.

Example Intelligence Requirements:

- Monitoring of any new technical change or new technology impacts.
- Monitoring of system performance and growth.
- Monitoring of organisational technical debt.
- Monitoring of daily backup and restoration events.

Setting Intelligence Requirement Priorities

By applying 4 R's analysis and building the 4 D's threat models for your organisation's services and products, specific intelligence requirements can be easily compiled. The greater the number of threat models, the increased number of information sources or feeds will be required to fill those intelligence requirements.

Some information will be easily available from public data sources. Whereas other intelligence requirements may only be fulfilled by technological solutions or bespoke information feeds. What is the best way to get this information to the CTI Program in an accurate and timely fashion, to provide actionable intelligence?

While an entire CTI program can be built using nothing but public data sources, the information may not be timely nor accurate. Additionally, due to the nature of some public data sources – such as social media – the credibility, integrity, and reliability of the information may vary widely. As indicated by your intelligence requirements, the monitoring of information related to your 4 D's threat models is of paramount importance. The better the information, the better the intelligence product will be. When a 4 D threat model appears more than once, with impacts to Revenue, Reputation, Regulation and Resilience – such as a major data breach – a bespoke information feed with high fidelity may be advisable. This will provide an actionable intelligence product, with reduced research and analysis requirements.

The Information Collection Plan

This is the final step in establishing your CTI program. The 4 R and 4 D process should result in a solid understanding of the information required to efficiently provide the business with a holistic threat intelligence product. The efficacy of this product is directly correlated to the amount of effort that is spent on acquiring reliable sources of information. In the same way that architecture is the foundation of robust IT systems, a CTI program is built on its Information Collection Plan (ICP). Perhaps the hardest part of developing the ICP is the enthusiasm to "Collect all the Things!".

An ICP for maintaining visibility on up-to-date information security news, for example, may include 48 Really Simple Syndication (RSS) sources and 40 or more information security social media influencers. It is not possible, or practical, to manually visit all these web pages and feeds. As such, an aggregation and central presentation of these findings are required.

Just like the 4 R analysis and the 4 D threat models, the ICP needs to be dynamic and responsive to organisational change. A sudden announcement of merger and acquisition activity can significantly impact the 4 R analysis and 4 D threat models – perhaps shifting the focus from production systems to the protection of Intellectual Property or a concern about the security of the council's office. The CTI program has to be able to adapt to a change in organisational priority and needs to have in-built flexibility.

What is a "flexible" ICP?

One of the most important outputs from a CTI program is not the intelligence product itself, but the feedback from the organisation on the timeliness and accuracy of the information and whether the intelligence product was actionable. If the intelligence product failed to meet expectations, it is likely that something in the ICP was lacking: a critical piece of information may have been missed; the hypothesis of the analyst and, therefore, the process of intelligence analysis, became misguided. Intelligence products are part of a CTI iterative process. If the output did not meet expectations, the ICP needs to be revisited. Since the ICP is derived from the 4 R analysis and 4 D threat models, then the problem is straight forward: you need more information on the poorly performing threat model.

Maybe the analysis is flawed, or the threat models have changed. The CTI program must revisit the analysis and re-apply the threat models (or create new threat models) to address gaps in the intelligence collection plan. Closure of those gaps will increase the chances the Intelligence product will be accurate, timely and actionable.

The Birth of your CTI Program

Start small and work from outside in. In creating a CTI program, the first place to start is focusing on the external attack surface of your organisation's IP addresses and domains. Applying 4 R analysis, creating 4 D threat models, and formulating an intelligence collection plan for "the outside of your company" is relatively easy.

For the purposes of this exercise, let's assume the 4 R analyses have determined that the organisation's revenue, reputation, regulations and resilience point to a single service. Clearly, that will never be the case, but for the purposes of this exercise, 'testcompany[.]com' has just a single exposure.

We can then move to the 4 D threat model:

- Disruptive threat model: no Disruption permitted critical if it occurs.
- Destruction threat model: backups of the website must be daily - ability to restore website is critical.

- Degradation threat model: performance of the website must be excellent.
- Deception threat model: website must be secure, and customers must land at the right website.

The ICP for the website may include:

- Telemetry for detection of an external DDOS attack on the website.
- Tactics, techniques and procedures (TTPs) for threat actors, which may target the organizations industry vertical.
- Understanding of all the technology components and subcomponents of the website.
- Monitor CVE, security research community and threat actor activities against technology components and subcomponents of the website.
- Monitoring of separate development, staging and production environments to ensure integrity.
- Monitoring authorized changes against change tickets, commits, or pushes from staging.
- Detection of unauthorized access and unscheduled changes to the production environment.
- Monitoring and review of the daily backup log.
- Test the restoration of website to the non-production environment.
- Monitor for registration of typo-squatting domains.
- Monitoring for hot-linked sites to your resources.
- Monitor for certificate issue and revocation for typo-squatting domains.
- Monitoring for certificate expiry for the website.
- Monitoring for changes or performance issues related to DNS, ISP, Registrar, and hosting infrastructure for website.
- Monitor SIEM, EDR, Load Balancer, front and back end services for unusual activity.
- Specific telemetry from bots conducting brute force and password spray attacks on website login portals or services.

As demonstrated above, the ICP for a CTI program safeguarding this one “crown jewel” website is likely to include multiple different internal and external data feeds.

The impact of the CTI program on your organisation

Good news in cybersecurity, compliance, audit and risk departments, is rare at the best of times. However, a tailored CTI program, using 4 R Analysis and 4 D Threat Models, built on a solid ICP, will provide proactive information that can be used to reduce harm or entirely avoid a major security event. Through this organisational preparation, it is possible to thwart cyberattacks before they have been launched.

About the Authors: *Ian Thornton-Trump, CD is an ITIL certified IT professional with 25 years of experience in IT security and information technology. Today, as Chief Information Security Officer for Cyjax Ltd., Ian brings to bear his significant experience concerning the threats faced by small and medium-sized businesses, and enterprises. His research and background have made him a sought-after cybersecurity consultant specialising in cyber threat intelligence programs for all sizes of organisation. From 1989 to 1992, Ian served with the Canadian Forces (CF), Military Intelligence Branch; in 2002, he joined the CF Military Police Reserves and retired as a Public Affairs Officer in 2013. After a year with the RCMP as a Criminal Intelligence Analyst, Ian worked as a cybersecurity analyst and consultant for multi-national insurance, banking and regional healthcare. His most memorable role was being a project manager, specialising in cybersecurity for the Canadian Museum of Human Rights. In his spare time, Ian teaches cybersecurity and IT business courses for CompTIA as part of their global faculty and is the lead architect for Cyber Titan, Canada’s program to encourage the next generation of cyber professionals.*

Zoë Rose is a highly regarded cybersecurity specialist, who helps her clients better identify and manage their vulnerabilities and embed effective cyber-resilience across their organisations. Zoë is a Cisco Champion and certified Splunk Architect, who frequently speaks at international conferences. Recognized in the 50 most influential women in cybersecurity UK for the past two years, and the PrivSec 200, Zoë is regularly approached for media comment, has presented on National News, been featured in Vogue Magazine, and was the spokesperson for Nationwide's Over Sharing campaign that had a reach of 306 million citizens.

[1] https://www.telegraph.co.uk/personal-banking/current-accounts/tsb-meltdown-leads-eight-fold-increase-customers-switching-accounts/

[2] https://nvd.nist.gov/vuln/detail/CVE-2017-5638

[3] https://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html

[4] https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

[6] https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

STATEMENT OF CONFIDENTIALITY

This document contains confidential trade secrets and proprietary information of Cyjax Limited. The recipient is expected to treat this document as they would their own confidential internal material. Neither this document, nor any diagrams contained in this document, may be disclosed to any person outside of the recipient's organisation without express written permission from Cyjax Limited. By accepting this document, the recipient affirms that they will comply with these expectations.

Cyjax Limited, Registered in England and Wales no 08302026.
Registered Office Suite 53 Peek House, 20 Eastcheap, London EC3M 1EB.
United Kingdom.

CYJAX
Cyjax Limited
Suite 53 Peek House
20 Eastcheap
London EC3M 1EB
info@cyjax.com
+44 (0)20 7096 0668
CYJAX.COM