Cyber Security Policies and Compliance for Business in the 21st Century

Policy Paper 2016

While the concept of reasonableness is somewhat subjective, the questions for CISOs to ponder are these: Does my security program constitute reasonable protections for a company in my industry and would the legal system agree? If my company is breached, and I have to explain my actions a year from now in front of a court, will those actions show that I did what was reasonable to protect my company's information assets?

1. Summary

Business communications have undergone a revolution; the new generation of workers have grown up with always-on Internet connectivity. This has driven a rise in real-time communications and messaging. These applications are now in day to day use in the business environment. Cyber Security Policies must adapt to this change.

- **Business and personal communication is changing**. There is a shift to real-time communications applications including voice, video and various forms of instant messaging. At the same time, the provision of these services is moving away from the phone network and these applications are now sharing IP network infrastructure with traditional data applications. Cyber security and compliance policies must be revised to accommodate this change.

- **Everyday real-time communication of data use is currently largely unregulated for consumers, but we are at a turning point for business survival** and while this remains the case, enterprises need to find a way of protecting their business and their employees whilst making the most of the opportunities gained from remote Smartphone and tablet computing via the internet over a public or private cloud computing environment.

- **Improper use of corporate data via real-time communication applications or social media can result in serious damage** to your business as well as the possibility of legal dispute and fines if compliance regulations are breached. Key risk areas include loss of valuable business assets, reputational damage and failure to meet regulatory requirements. A compliance failure can result in penalties of up to 4% of annual turnover, with higher penalties if the breach is the result of poor cyber security planning.

- **High risk businesses that are singled out for special mention by authorities (Network and Information Security Directive-NIS) can protect their information** by implementing clear cyber security policies. The recent European Union General Data Protection Regulation (GDPR) extends and strengthens the regulatory requirements which now apply to all businesses processing personal data.

- **Applying clear policies and monitoring the use and performance of remote Bring Your Own Device (BYOD) and or business paid device usage,** will help minimise the risks to your business and improve your chances of enforceable legal protection. Where employees ignore and breach policy and contractual protections, employers should consider taking appropriate action to safeguard their business interests.

- **Real-Time remote communications of data and information can offer great opportunities for businesses** to develop their own solutions to engage with customers, offering brand building, more focussed content and communication, data ownership and control and reduced reputational risk. For many, the ideal solution could be to purchase an overlay cyber security cloud service or use a developed and extended set of cloud services either in a public or Hybrid cloud, which has appropriate automated links from all technology employed, such as PBX, UC systems, Customer Service Centres and all mobile connectivity.

- **Cyber-attacks are now common place which suggests that there is a mirror of the corporate value chain at work,** the underground cybercrime community is built on anonymity, and this anonymity drives a grey free market system. The actors are known only by their handles; their true identities remain hidden. This breeds a strong paranoia throughout the business. Trust and a good reputation are key to the industry. If you are not trusted, it is very difficult to make money in the system. It is clear that having a well-defined and comprehensive cyber security policy is one of the criteria a regulatory assessor uses to measure the effectiveness of the business' security controls. These controls must be designed against a recognition of this mirror value chain, so to defend against the threats and maintain the compliance now forced upon the board of directors.

2. Introduction

Our increasing reliance on fast and efficient communications in both our business and personal lives increases our exposure to cyber threats. These threats are nothing new. Since the emergence of the World Wide Web in the early 1990s and the growth in the use of Internet based email services we have become accustomed to the fact that connectivity brings both benefits and risks. Whether we have taken effective steps to control those risks is another question. The new generation of real-time communications applications are potential targets for the existing cyber threats but also introduce new threats. This review covers both sets of security threat.

Businesses need faster forms of communication to improve productivity and reduce costs. The new generation of workers are turning towards familiar applications to achieve this. These new applications include IP applications for voice (VoIP) and video calls, conferencing services and messaging. These are made more effective through the use of presence services, the ability to track the availability of colleagues. These new services have developed in the absence of clear controls and regulation, exposing the business to new cyber threats. However recent moves by governments both in Europe and North America are pressuring business to ensure that their security policies cover all methods of data processing and communication.

Europe is taking a lead on this initiative. In December 2015, the European Union published the General Data Protection Regulation (GDPR) (European Parliament, 2016). This builds on previous EU initiatives, including provisions for data erasure (right-to-be-forgotten) and data portability. To assist businesses in meeting the new regulations, the European Union Agency for Network and Information Security (ENISA), have published a set of technical guidelines. These guidelines specifically include the new generation of communications services and extend to the networks commonly used by those services (public WiFi, 3G/4G, VoIP services).

Government has been understandably reticent about regulating real-time communication, until it became a risk to commerce and trade with Cyber Crime growing to a level that represents a real threat to data privacy and has significant economic impact. Board level ignorance is no longer acceptable. While the concept of reasonableness is somewhat subjective, the questions for CEO, COO and CISOs to ponder are these: Does my security program constitute reasonable protections for a company in my industry, and would the program withstand legal scrutiny? If my company suffers a security breach, and I have to explain my actions a year from now in front of a court, will those actions show that I did what was reasonable to protect my company's information assets?

Thus it is important to have a set of rules that show the value chain working from cyber security protection upwards through to compliance and policy directives. The resulting cyber security policy must be clear and concise, understandable and acceptable at board level and most importantly able to demonstrate that all reasonable efforts had been made to protect against cyber threats. In the event of a security or compliance breach, the ability to show that the organisation's cyber security policy recognised the threats, used the most appropriate available technology to protect against those threats and that the policy was fully implemented, is an effective method to reduce the penalties imposed by the data protection authorities.

Take a lead, self-regulate and provide support to the business, large and small, in addressing this challenging and dynamic environment. This Paper is designed to help business leaders develop informed cybercrime policies which are effective in protecting the business and ensuring conformance to compliance regulations.

The New Communications Paradigm

The communications revolution gathers pace - never before have so many people communicated so much so often.

Generation Y and Generation Z will automatically use instant messaging rather than email, text messaging rather than voice calling, video calling rather than face-to-face meetings and share personal data about their lives in a page on a social network.

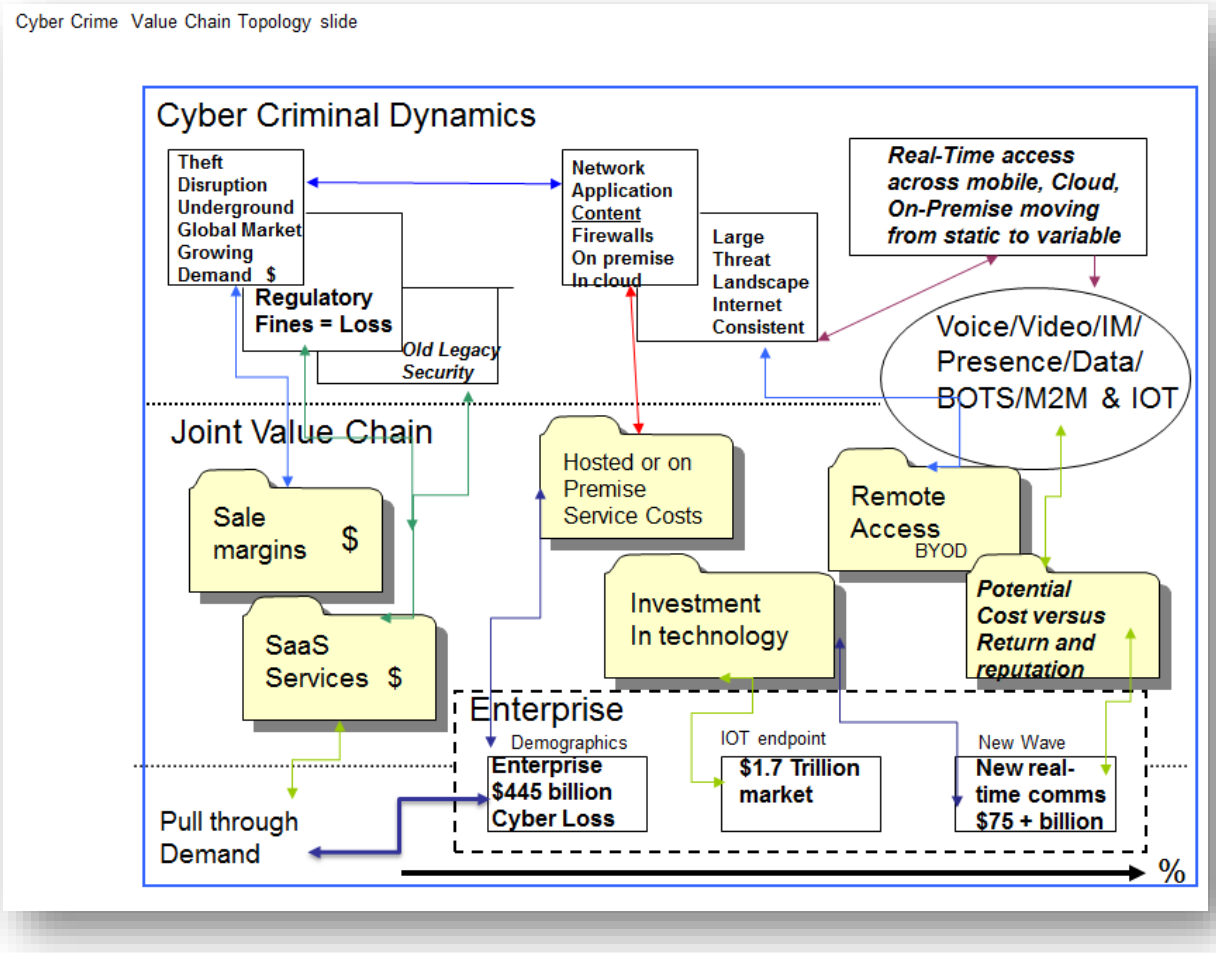
Messaging is the new phone call, so it would appear, as ‘WhatsApp’ has demonstrated by surpassing 900 million active users every day, but only recently providing encryption for their traffic as a way to prevent breaching the confidentiality of personal data.

Like it or not, the business world is well and truly online and inextricably linked with this communications revolution. All this can be considered progress, but the rules of engagement in this brave new world are far from clear. Technologies provide the tools to achieve real-time communications, delivered by multiple companies, but not all products are inter-operable and not all are able to protect against cyber-attacks. Multi-vendor systems are the reality, but mixing products where some have limited security controls makes providing 'end-to-end' compliant cyber security a challenge.

Good business management requires clear strategies for successful online engagement, with clear guidelines and policies to manage potential risk to companies and their employees.

Broadly understood, compliance is an important mechanism that supports effective governance. Compliance with regulatory requirements and the organization's own policies are a critical component of effective risk management. Monitoring and maintaining compliance is not just to keep the regulators happy, it is one of the most important ways for an organization to maintain its ethical health, support its long-term prosperity, and preserve and promote its values.

3. Cyber-crime value chain



Hacking is a business. The most effective way to disrupt this business is to increase the cost of each attack, to erode the attacker's profits and increase the time it takes to successfully execute an attack and gain a financial benefit. Businesses must design their cyber security policies with this goal in mind. The polices and the cyber security defences implemented as a result of those policies must include the best available technology which will provide the most effective method of detecting and blocking attacks and disrupting the attacker's value chain.

A value chain is a set of activities performed in order to deliver a valuable product or service to the market. These activities are carried out by subsystems that take an input, process it in some way to enhance value, and provide an output. All these activities together give the output more added value than the sum values of the individual activities. The effectiveness of the value chain determines the cost of the output and affects profits.

The series of activities in the value chain of the business of hacking are not under an organizational umbrella like a corporate enterprise. However, they are all pieces that contribute to the end product. This is a deeper look into the primary and support activities involved in “the business.”

Most successful hacks are complex and are executed in stages. To follow the business model analogy, the driving factor is an identified financial gain or other advantage. This may be a direct and immediate gain, for example making fraudulent calls, or a delayed advantage, for example disrupting the victim’s business. In many cases the motivation behind the attack is not immediately clear. The attacker may believe that they are initiating the attack for altruistic reasons.

Whatever the motivation, the next step is for the attacker to identify the target. In some cases, the attacker has a specific target in mind. In others this step becomes a fishing exercise, searching for a target where poor security enables the intended attack. Hacks with the goal of financial gain fall into the second category, the attacker's only preference is that the subsequent hack should succeed.

The final step in the hack is the attack itself. This means breaching whatever cyber defences are in place and compromising the target system.

An effective cyber security policy needs to recognise this staged approach by understanding the possible targets and their value to an attacker and by implementing a set of security controls which offer effective protection. These security controls must be multi-layered to recognise and block the attacker's fishing expedition and to back this up with robust defences to prevent the attacker's follow up actions. Each security layer must include auditing and alerting functions to enable early threat detection.

4. Compliance

On a more practical level, a compliance program supports the organization's business objectives, identifies the boundaries of legal and ethical behaviour, and establishes a system to alert management when the organization is getting close to (or crossing) a boundary or approaching an obstacle that prevents the achievement of a business objective.

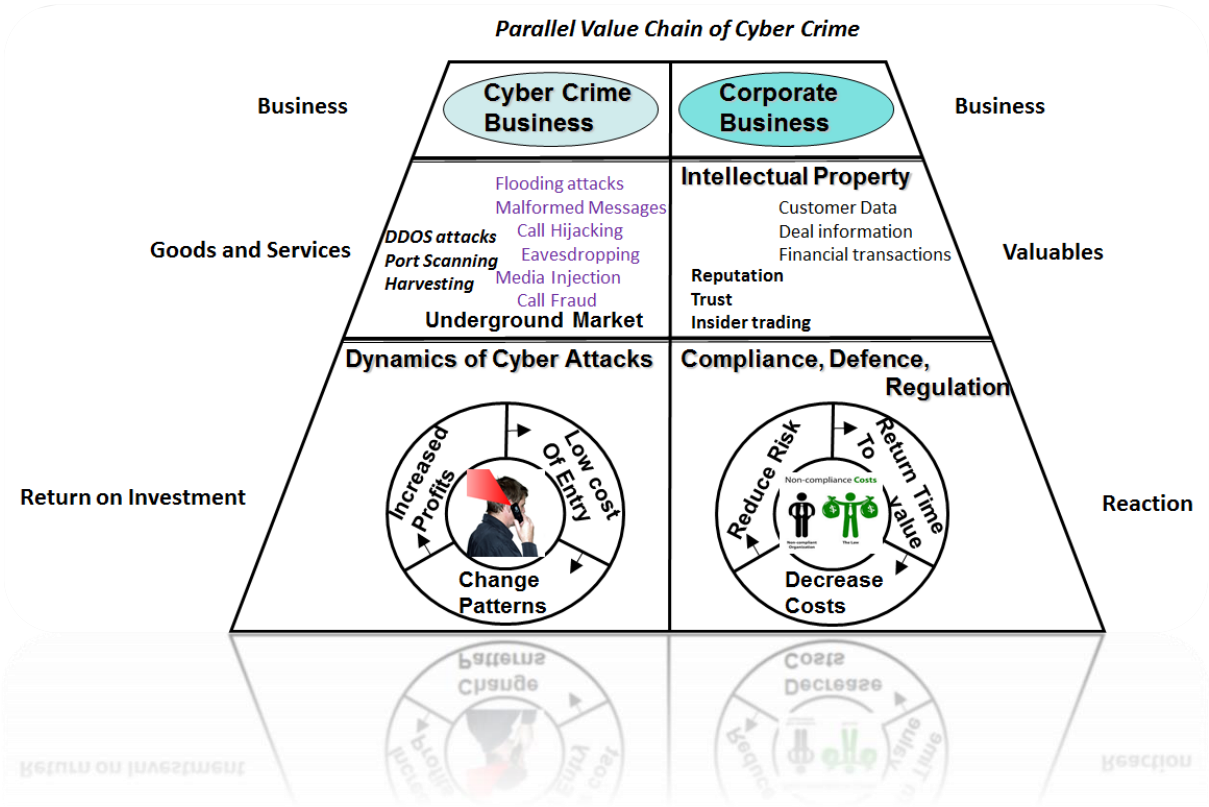
Once an issue is detected, management must be prepared to respond quickly and appropriately to minimize the impact on the organization (and the community, as appropriate).

A well-designed compliance program is only half the picture. Compliance programs must operate against a background of constant change, increasing complexity, rapidly evolving threats and the need for continuous improvement. A successful program requires organizations to have the commitment of senior management and the board, adequate authorization and funding, the appropriate tools to monitor the effectiveness of security measures introduced to meet the compliance targets and a method of utilising threat and intelligence information generated.

Implementation is often the most difficult aspect of any program. This is where most failures occur. However, if executed well, a structured rules based approach provides an opportunity for positive influence on the organization's performance and culture.

Compliance practices can no longer be viewed in isolation from the rest of the organisations or viewed as a necessary evil to keep an organization out of jail. It must become part of the overall business strategy and operations, pervasive throughout the entire organization. Ultimately, taking this integrated approach will lead to better overall performance and compliance will become less of a burden on the business.

The cybercrime value chain and corporate business value chains mirror each other. A side-by-side comparison provides an effective mechanism for both management and employees to visualise the similarities.



Compliance risk is the current and prospective risk to earnings or capital arising from violations of, or non-conformance with, laws, rules, regulations, prescribed practices, internal policies, and procedural standards.

Compliance risk can lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and an inability to enforce contracts.

The 21st century has seen a change in the way businesses communicate, influenced by changes in personal communication.

Personal Publishing. Although the direction of communication is principally a broadcast from the author, interactivity is enabled via comments from other readers and sometimes the facility to rate an item. Content may be shared more widely via a variety of social mechanisms including bookmarking services. These functions are intended to promote collaboration and improve communication, but as a side effect can breach the compliance rules protecting personal data. Without clear guidance and education, users can inadvertently leak classified information or compromise intellectual property.

Social Networking. For many this term is synonymous with LinkedIn which has become the industry standard in many parts of the world. For leisure and consumer purposes this space is dominated by Facebook. Users connect with others via their social profiles and are able to establish a unique personal network to which they can send updates and from which they can observe activities of their contacts/friends. It is a people-centred environment rather than content-centred and this "social" model is already being viewed as a central component for more effective working inside organizations as well as for keeping in touch with contacts.

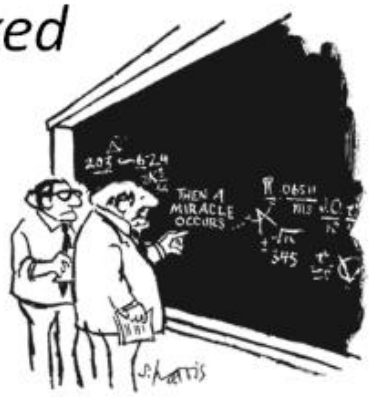
Open Collaboration. Possibly the most exciting aspect of social media has been the ability for groups to work together more effectively and co-create IP for the good of the wider community. In stark contrast to the owned documents of the Microsoft era, tools like forums, wikis and more recently Q&A environments have opened up communal collaboration. The most widely used examples of these are the close-knit communities in LinkedIn Groups and Facebook Groups. Successful groups can quickly become large communities in their own right. At the business level, an open and free Google Docs has triggered the emergence of a new method of information sharing and collaboration, one that leads to new cybersecurity threats and compliance requirements.

Risk IT strategies and investments over the business period will remain critical as policymakers around the globe stay focused on capital buffers, trade transparency, accounting and reporting improvements. In parallel, internal control and IT system continuity, third-party risk, financial **crime and fraud**, and the impact of **cyber threats** on the safety and soundness of the business and country economics are all aspects of rules to be included in a common companywide cybercrime policy. Three Tier attack models are directly aligned to the value chain of the underground market for cyber-crime; in all cases it should be considered a stepping stone in process by the cyber-criminal to achieve the most valuable assets by moving up into the content that returns the most profit for the cyber-criminal and this is achieved from multiple areas of the attack surface becoming opened up if not properly protected across all layers.

Reporting on personal data breaches, another important element of GDPR is the notification of personal data breaches. In the new framework, this obligation extends to all sectors, going beyond its current applicability to the telecom operators; see for example the EU's ePrivacy Directive (European Commission, 2016). This new obligation is an accountability measure for the corporate that, on one hand needs to take all the necessary security measures to avoid data breaches and on the other hand has to notify these breaches to the competent authorities and to the affected individuals.

Are you ready to be tested?

Hacked



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

"Answer is compliant service design and management", but is the customer ready for compliance and testing – then to gain from this?

5. Areas needing protection

There are a number of areas for a corporate CISO to consider regarding managing business risk.

Business value. A substantial part of most businesses value is derived from their intellectual property, client contacts, financial status, specific deal making and overall strategy. To protect these assets business must ensure that:

- Protection is in place to retain ownership of all without it being hacked, disrupted or affected by loose employee activity
- The security measures are comprehensive and will protect against all of the identified threat levels.
- Employees are aware of their responsibilities for recognising the value of business assets and their responsibility for protecting this value.
- Employees are aware of the corporate standards for information processing and communications and the relevance of those standards to safeguarding business value.
- An effective policy is in place to define and manage the security measures and employee responsibilities.

Failure to do so may lead to the business losing significant value if a breach occurs or regulatory fine is imposed. Value can be lost if a potential buyer may consider lowering its offer price for the business if the security policy or the management controls are regarded as inadequate. Finally, public shareholder value may be impacted.

Brand & Reputation. It is important that business policy and strategy is properly represented online so that all communications and responses are aligned with the business and legal or other issues are avoided. This can be particularly challenging in fast-moving and/or high-profile scenarios, where even quite small incidents can quickly mushroom into major PR incidents.

Regulatory issues. An organization can implement processes and security measures that comply with the legislative requirements for the security of electronic communications of the European Union. HR 1770 (Blackburn, 2015), the Data Security and Breach Notification Act of 2015 in the USA along with the EU Directive 95/46/EC, now the new General Data Protection Regulation in Europe, presents major milestones for Cyber Security compliance.

It also requires service providers, Enterprises in high risk areas (NIS -Finance, Government, Oil and Gas, Health etc.) and their service providers to alert breaches of data to the authority list within 72 hours in Europe. If found to have not aligned to the guidelines on security technology defences and compliance rules, a fine of up to 4% of annual turnover or €20 Million (whichever is the greater) is attributed to the increased costs of doing business.

Businesses whose staff deal with customers via real-time communication and social media may be conducting regulated business in a non-protected environment. Is sensitive personal data being collected and stored for the employer on a networking site? Without the appropriate compliance and cyber security controls, this could breach GDPR. What about sales activity via social networking sites, IM and Video exchanges where such activity is subject to strict regulation such as NIS services? Allowing employees to operate via new media, outside the

normal IT systems of the employer may place employers in serious breach of various regulatory regimes, so having a rules based transparency becomes crucial to protect the employee and company.

Confidential Information. In many situations advice or expertise may be shared and care must be taken to avoid inappropriate sharing of commercially sensitive or confidential information. Informal communications online, via remote smartphone or tablet access, can be seen by infinitely more people and again are easily accessible in the attack surface for a cyber-criminal. Safeguards must be in place to ensure all employees have clear knowledge of what can and can't be discussed online, whether or not they have outward facing responsibilities.

Intellectual Property. Social media, video calling, presence tracking communications may also include images and media materials which have been created by the business. IP owners should assume these will be widely shared. Consequently, steps should be taken to implement appropriate branding and disclaimers to cover as many potential usages as possible. Re-use can have many advantages but this needs to be protected by appropriate copyright and brand protection.

6. The need for Cyber Crime protection policies in the work place

Best practice advice says: Businesses of all sizes should have a properly drafted policy ensuring compliance to the regulations applicable to their business and industry sector and use of their BYOD and computer systems. The cyber security policy should analyse potential threats and clearly document the security controls implemented to protect against those threats. The threats, particularly those affecting applications delivering real-time communications services, can be categorised in 3 layers:

- Network level threats. These threats include generic threats which affect all network applications. Traditional approaches to network security, such as generic firewalls, focus only in this layer.
- Application level threats. These threats target vulnerabilities specific to each application. Examples include call termination and call hijacking attacks against VoIP and UC applications.
- Content level threats. These threats expose communication content and include unauthorised monitoring of voice or video calls and Instant Messaging services.

The policy must demonstrate an understanding of the threats at each of these levels and consider the requirements of a geographically dispersed and mobile user population.

The policy should include a specific, express waiver by employees to any right to privacy in information contained on the company data storage, either cloud or on premise computers. The policy should also eliminate any expectation that information or communications are confidential to the employee and acknowledging the employer's right to access their mobile smartphone or computers at any time to review and monitor the contents.

However, employers should restrict this access to occasions when there are valid business reasons for doing so, such as when there is a reasonable suspicion of work-related misconduct by the employee or regulated activity which the employer has a duty to monitor.

Employers should also consider clearly stating that all computers owned by the business are company property and should not be used in any disruptive or offensive ways, such as communicating sexually explicit content, ethnic or racial slurs, or to discriminate, bully or harass others. Employees should be notified that their employer deems all computer content permanent and subject to retrieval and review at any time.

European Union Agency for Network and Information Security (ENISA), regularly publish a Threat Landscape Report (ENISA, 2016). Their most recent report provides an overview of the range of security threats faced.

Malware

Apps and consequently app stores remain a primary target for "packaging" and spread of malware. There have been successful attempts to overcome vetting processes of official app store. A recent Apple store hack has affected possibly thousands of apps, potentially used by hundreds of millions of users. Android app stores suffered similar incidents in 2015/16 period. A technique for patching existing software and introducing malicious code has become the main method to distribute Trojans.

Web Based Attacks

A view on web based attack statistics unveils important details behind web based attacks. Top five categories of web sites exploited are: technology, hosting, blogging, business and anonymizer (i.e. services providing anonymity). The most common threats found is browser exploit, followed by virus and phishing. While clicking on mailed malicious link is also considered as belonging to the top infection vectors. Malicious URL is considered to be the second on the top 20 list of malicious objects online.

Web Application Attacks

It is worth mentioning that attacks tactics differ among web applications found on web pages and mobile applications. While in mobile applications attacks are based on the quality of code, attacks on web pages' abuse more often the environment of the application. On the other hand, abuse of errors (i.e. error code messages) is an attack method mainly surfaced in web applications. However, the general trends regarding attacks are similar in both web and mobile applications: abuse of APIs follows abuse of environment and abuse of security features. Statistics go along the lines of generally assessed vulnerability likelihood of web applications. It is found that the top positions: transport layer protection, information leakage, XSS, brute force, content sniffing, cross-site request forgery and URL redirection.

Botnets

It has become clear that botnets (networks of compromised systems under central control) are one of the most important business cases for cyber-criminals (aka botnet-for-hire) and the main element in cyber-crime consumerisation (Value Chain). To this extent, botnets are the first item that has reached market maturity in the area of Cybercrime-As-A-Service. In the reporting period we have seen prices between USD 20 and 40 for one hour per month DDoS attacks performed via botnets, aiming at increasing attack amplification/attack bandwidth. The fact that between 20% and 40% of the DDoS attacks have botnet fingerprint, is indicative for the level of adoption of botnets for cyber-attacks. Enabling big impact attacks at low costs is the main driver for the increasing use of this tool. At the same time this is a major concern of cyber-security business users.

DoS and DDoS Attacks

Denial of Service (DoS) and attacks and the related Distributed DoS (DDos) attack typically flood a system with network traffic, disrupting the service that the system is intended to provide. The growing cyber-crime tools market provides DDoS-as-a-service offerings. Depending on bandwidth and attack mix, prices from ca. 20USD to 40USD are common for ca. 1 hour per month usage of DDoS botnets. There is evidence that ca. 40% of the DDoS traffic is generated by such DDoS-for-hire offerings. It is important to underline that such services deliver to any non-specialized individual tools to perform powerful DDoS attacks at affordable prices. This fact introduces a risk potential to IT infrastructures and services that is very difficult to calculate.

Studies performed, have provided an insight into the impact of a successful DDoS attack and the subsequent costs. The studies found that two thirds of victims had temporarily lost access to critical information, one third had been unable to carry out main businesses and another third had lost business opportunities/contracts. The costs of DDoS attacks have been calculated at $40.000 per hour, while average costs of successful DDoS attacks may range from $40K to $500K. Approximately one third of respondents calculate costs of between $5K and $20K per hour. Costs are proportionate to the company size. These figures remediation costs incurred after a successful attack.

Phishing

Obviously, user habits are decisive for the failure or the success of phishing mitigation. It has been argued that user awareness may achieve ca. 5-10% phishing detection. On the other hand, phishing tactics are decisive for the success of a campaign: a slow, persistent campaign that includes some messages leads at a rate of 90% to a success. Obviously this is a spear-phishing-like attack tactic. On the other hand, untrained users are falling victims of phishing campaigns irrespectively of the awkwardness of the malicious URL.

SPAM

Spam, one of the oldest cyber-threats, is still a “baseline” tool for cybercriminals. Although spam is in a declining trend since some years now, its importance in the malicious arsenal remained at least almost equal: new methods of “weaponization” of this threat make it a serious threat. It has been assessed that spam is an effective means for malware distribution. Ca. 6% of overall spam volume included malicious attachments or links. Moreover, malicious Office documents and ransomware were among the distributed malicious objects.

Exploit kits

Software tool kits designed to enable attackers to take advantage of known security vulnerabilities, they are now a primary mechanism for malware weaponization, delivery, exploitation and installation of malware. Exploit kit use-cases and deployment models vary according to roles taken or agreed upon by cyber-criminals in the attack lifecycle. For example, exploit kit developers might establish a cooperation with the user of the kit, if they are allowed to deliver own malware, hence indirectly co-profiting from the launched campaign.

Data Breaches

Identity information is number one breached data type (over 50%). This is the reason for looking at related cyber-threats separately. Identity loss is followed by loss of financial access information (credentials) (over 20%), followed by existential data (confidential data or intellectual property) (over 10%) user credentials (over 10%) and nuisance data (3%). Top three affected sectors are government, health and technology (making up ca. 80% of the breaches). Some spread in statistics can be observed regarding the sector education (2nd position with ca 14% of breaches vs. 7th position with ca. 7% of the breaches).

Identity Theft

According to regulation bodies both in the USA and Europe, personally identifiable information consists of any combination of: Full name, Home address, Email address (if private from an association/club membership, etc.), National identification number, Passport number, IP address (in some cases), Vehicle registration plate number, Driver's license number, Face, fingerprints, or handwriting, Credit card numbers, Digital identity, Date of birth, Birthplace, Genetic information, Telephone number, Login name. Access to ID is crucial for all forms of level 2 and level 3 attacks.

Ransomware Attacks

Defence regarding ransomware should be MULTIPLE LAYERED oriented. This is because just like most of malware, ransomware infections happen at content and application user level. Given that end-point virus protection cannot defend all possible infection vectors related to this threat, additional defences need to be included. Nevertheless, focus of defence controls is always the end-user, that is, they need to be Multi-layer centric. This does not mean parallel defences thwarting important cyber-crime infrastructure components should left out of focus, but legacy defences such as Session Border Controllers, Firewalls, VPN, Gateway Proxy and MPLS do not have an integrated approach to deal with this attack surface.

The recovery from a ransomware infection is generally not possible. Encrypted data can only be recovered via the use of cryptographic key used by the malware. And usually this is at the possession of the cyber-criminals. So to establish all data as Encrypted in the first place would prevent knowledge of data held to ransom.

Much of the last decade will have been about protecting static data models from attack via various hardware designed technologies (legacy), today the 21st Century Real-Time communication platform and social media services are testing the defences of all businesses and in this, require new design methodology for cyber defences that mirror cyber-criminal approaches.

The evolution of business communication towards an increase in the use of real-time communications has generated a new set of threats specific to the protocols and applications that drive real-time communications.

Real-Time Communication DoS

A new category of DoS attacks which rely on a single protocol request rather than the flood of traffic employed by standard DoS attacks. This new form of DoS attack is more difficult to detect and block than standard DoS attacks and the countermeasures that are employed mostly rely on detecting and blocking large volumes of network traffic. These countermeasures are ineffective against the new generation of DoS attack.

Malformed Messages,

Application specific threats with a range side effects including turning a phone into a bugging device of causing an entire call centre to crash.

Call Fraud

Call fraud has been a problem since the first phone networks were installed. Moving voice and video telephony to IP networks has magnified the problem as attackers can exploit the power and flexibility of IP networks to locate a target system and launch an attack from anywhere in the world. An attack which is growing in frequency is the International Revenue Share Fraud (IRSF). An attacker first sets up a premium rate number and then scans the Internet using readily available tools to locate a poorly protected VoIP system. The attacker then forces that system to make multiple calls to the premium rate number and collects a share of the revenue. The cost of a successful attack can run into tens of thousands of pounds.

Eavesdropping

One of the benefits of the new generation of real-time communications applications is the ability to remove the physical barriers of communication. A user can receive or make a call from anywhere. The same IP technology that delivers that benefit carries a risk. Unless the appropriate countermeasures are in place there is a risk that the call could be monitored by an unauthorised 3rd party. In some jurisdictions, this 3rd party could be a government owned or controlled phone company. If a call is monitored, then the privacy and integrity of any confidential information exchange is compromised; a clear compliance failure.

Call hijacking

This attack misuses a standard function of most VoIP and Unified Communications systems, the ability to transfer or forward a call. By monitoring a call, an attacker is able to construct and inject the protocol requests to insert himself into an established call or to disconnect one of the parties and take over the call. The risk potential is large. As an example the attacked could hijack a call to a banking service immediately after the authentication process had been completed.

Media Injection

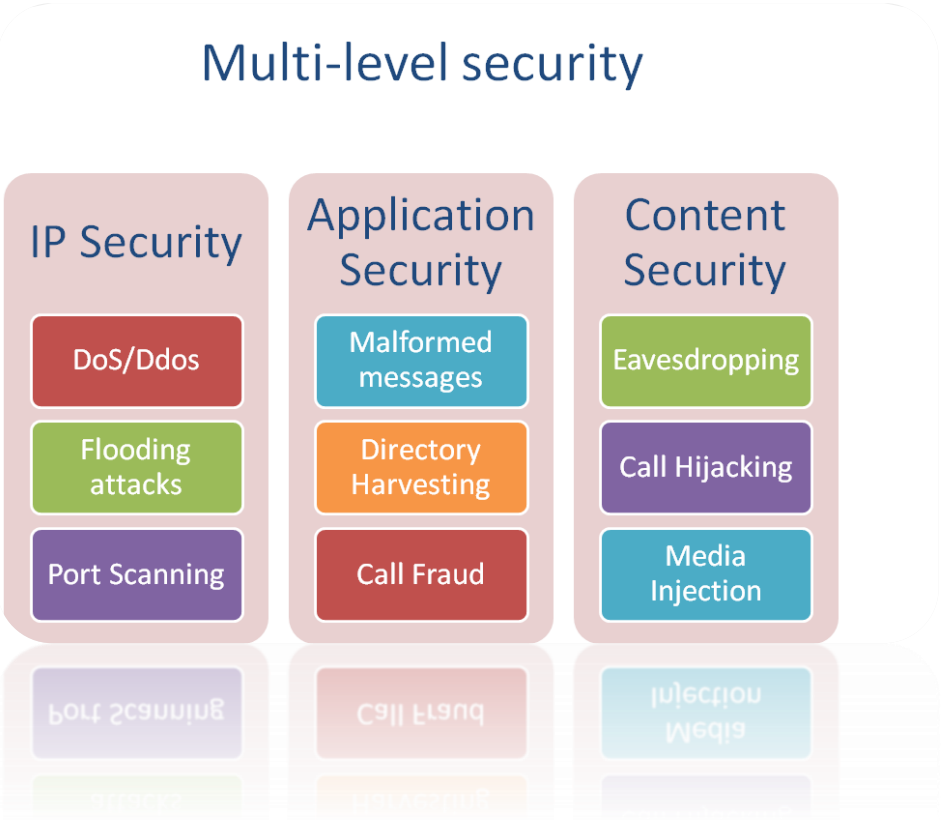
While most real-time communications applications include functions to authenticate and verify a user's request to set up a new voice or video call, many systems fail to validate the media streams (voice of video) set up for that call. This enables an attacker to inject and alternative media stream into an established call. The consequences range from the user's application crashing, to the call terminating because the application is unable to handle both the legitimate and injected media streams.

Real-Time communications will continue to be a significant challenge as it will now include Internet of Things (IOT) from which the cyber-criminal will build new business offerings. It is expected that by creating a multi-level, multi-tiered defence structure, this can be extended to cover IOT and Network of Things (NOT) in the near future as attacks are established.

7. 21st Century Security Technologies

In parallel with the evolution of new applications and the emergence of new security threats targeting those applications, innovative R&D companies have developed new security technologies to counter those threats and to enable businesses to define and implement an effective set of cyber security controls. The availability of security technologies proven to secure the applications used in support of business communications in the 21st century support the definition and implementation of an effective cyber security policy.

The cyber threats are multi-layered; security technologies need to take a multi-layered approach to project against those threats.



The deployment of any security countermeasures must be validated and monitored with a structured testing program.

Effective audit and test scenarios

Cyber security threats affect a wide range of applications; any cyber security policy must address the threats across the range. An important part of any policy is to establish a program of testing and validation of IT systems. Both the policy and program must cover application specific threats and consider the services delivered by those applications. One of the more challenging areas to define a policy is the relatively new field of real-time communication. A more detailed analysis of the requirements of real-time communication serves as a good model for other application areas.

Real-time communications require a new form of cyber security. The security controls developed for legacy communications applications (e.g. Web and email) do not provide effective security for the new generation of applications. New security measures are needed and new testing and auditing methodologies are needed to validate them. The security measure and testing methodologies must together be able to demonstrate compliance with current regulations, including the EU's General Data Protection Regulation (GDPR). To assist in interpreting and implementing GDPR, the European Union Agency for Network and Information Security (ENISA) published a set of guidelines.

The General Data Protection Regulation is an important step forward for enhancing privacy of EU and trading partner citizens, harmonizing data protection rules across Member States and trading partner countries, and promoting privacy and security as core aspects of the European industry. ENISA is already well positioned in order to provide valuable contributions that support the proper implementation of crucial aspects of the GDPR during the two years' transition phase before its application.

ENISA's technical guidelines provide a useful staring point to define a test and audit program. Taking these guidelines as a starting point, program for real-time communications applications should include the following.

Full audit and testing including: -

1. A detailed analysis of the security provided at the network level, specifically the system's ability to protect against network level flooding attacks from real-time traffic across multiple transport protocols (UDP, TLS, TCP)
2. An analysis of the application level security. This should be validated with standard testing tools appropriate to the applications under analysis, such a RFC 4475 for VoIP and UC applications
3. An analysis of the system's ability to protect against application level flooding and DDoS attacks.
4. An analysis of the system's ability to protect against password guessing attacks and directory harvest attacks.
5. An analysis to test the system's Call Admission Controls (CAC). A well designed security product will be able to limit calls and other SIP messages by message type, source and volume.

6. An analysis of the system's ability to protect against call fraud by employing the industry available tools used by fraudsters and value chain.
7. An analysis of the system's ability to control the available Session Initiation Protocol transports and to limit the available transports based on network connectivity.
8. An analysis of the system's ability to provide effective media encryption.
9. An analysis of the system's ability to detect and log attacks and to provide the audit information needed to meet compliance requirements.

Successfully designing and executing a testing and audit program that it appropriate to the services and applications provided, can be a complex task requiring specialist assistance.

Extra considerations for testing and audit set against public platforms are: -

The terms and conditions or a platform's usage policy on social media platforms such as Facebook, LinkedIn and messaging apps, can and do change quite regularly and, of course, the user has no recourse other than to stop using the service. In many industries the user would have to consider what impact could this have on their business.

Businesses should not assume that service will remain constant, these are still relatively immature business models, so substantial changes may be ahead. It is unlikely that legislation would be introduced to limit change, which means that the clearest route to resisting such change could be on the grounds that the platform's actions are anti-competitive or in restraint of trade.

Another consideration for every social platform is that they can be abused by third parties in a variety of **legal and illegal** ways. Programs can replicate user behaviour and, armed with a valid user account, quickly and efficiently access all available contact accounts and harvest their data. Businesses cannot assume that online services provide any guarantee of security:

"***That profile, that picture, that browsing habit or that buying pattern makes this generation the easiest and more importantly the quickest, target for fraudulent misuse of identity since the practice began***." *Computer Fraud and Security-Reed publication.*

Individuals and business leaders must understand and accept that it is an imperative for any online service to be able to supply their services and cover their costs while making a profit for their shareholders. We can benefit from these services but we should not presume they are mature, stable or secure. Whilst money may not have changed hands, your participation in the service represents a level of investment and "caveat emptor" still applies.

8. Where Next?

Steps to Ensure Real-time Communication Compliance

As we have seen, compliance obligations extend beyond basic technology solutions and basic management of resources and are about more than implementing either a call recording application or a training course.

Compliance also requires that systems used for information processing are protected against attacks that could result in information leakage and loss of confidentiality of personal information.

Personal data must be kept safe and secure from potential abuse, theft or loss.

The EU's GDPR backed up by the ENISA technical guidelines sets the current compliance requirements. If an organisation processes any personal data, which includes basic information such as contact and payment details for customers, then that organisation is responsible for ensuring the safety of this data. The specific financial sector regulations may also apply. In both cases the compliance requirements apply to both data and Real-Time communication services the latter including all voice, video, presence and IM communication.

Compliance for Real-time communications is a process, the key steps in this process are:

1. Understand which of the many regulations apply.
2. Audit your platforms, Social Collaboration and telephony systems to ensure that they are adequately protected from attacks that could lead to the compromise of personal information. This audit should check for both generic network security vulnerabilities and vulnerabilities specific to the protocols used.
3. Review your existing security measures, recognising that most IT data security measures (Firewalls, VPNs etc.) do not adequately protect UC applications.
4. Review the need for call encryption, particularly for mobile devices used to communicate sensitive information.
5. Review the need for call recording, any financial sector organisation subject to MIFID will need to implement this if not already obliged to do so by other regulations.

Unified Communications services are blurring the boundary between data applications and telecom services. As a result, many telecoms providers are now examining these services to ensure that service provision remains within the compliance framework imposed by national or supranational governments.

As a result of over three years of research and successfully completing many security and audit tests in both enterprise and carrier networks, UM Labs has developed an expertise in this area. The company has also developed a security platform designed for deployment in public and private cloud services to ensure that the security and audit requirements for real-time communications are met. These are:

1. To protect from attack on three levels, network, application and content.
2. To protect the UC systems from attacks, including Denial-of-Service (DDoS) attacks. See the UM Labs white paper, *Combating Denial of Service Attacks for VoIP and UC* (UM Labs, 2014) for further details on DDoS attacks.
3. To provide auditing functions to record all attacks on the system and to record the corrective action taken.
4. To provide alerts when the system is attacked.
5. To provide encryption services to protect voice, video and IM communications.
6. To enable the recording and secure storage of calls, including encrypted calls, to meet compliance and legal intercept requirements.

What should a Cyber Security policy cover?

The absence of clear rules surrounding employee use of BYOD and social media can cause problems for employers needing to take action against misuse. If an employee is dismissed due to their use of BYOD access on corporate data and social media, there is no clear policy in place, there is a risk that the employee may bring a claim for unfair dismissal against the employer. This is why it is essential that a carefully worded policy is teamed up with the employer's disciplinary policy. Given the importance and implications of these policies for recruitment businesses they should be reviewed by specialist advisors with experience of advising businesses.

A high-performing compliance program is best organized as an integrated capability assigned to business functions/units while managed and overseen by individuals with overall responsibility and accountability. Compliance can be a daunting challenge, but it is also an opportunity to establish and promote operational excellence throughout the entire organization and significantly improve the overall operational performance.

A Cyber Security policy should set out:

1. The risks (to the employer and employee) attached to accessing corporate data while unencrypted and not using a proven and approved security application on the BYOD or using a fully protected corporate device while accessing corporate cloud infrastructure;
2. What is, and what is not, acceptable in terms of references to the employer in communication;
3. Staff requirement to back-up online contacts and member lists from any back office by requiring them to submit such information to central storage on a regular basis;
4. That the employer will take disciplinary action against employees who use real-time communication tools and social media in a way that is potentially damaging to the business;
5. Rules on accessing all real-time communication tools and social media during working time;
6. Measures that an employer will take to protect confidential information relating to clients

Rules and guidance relating to employees' use of real-time communications and social media to promote the business in the course of their work, including ownership of data.

It is important to consider how "confidential information" is defined within the employees' contract of employment and whether this covers client contact data, corporate intellectual property other employee data. Restrictions should also be imposed on an employee during and for a limited period following their employment to prevent them from using confidential information at a competitor/opposing organisation or to set up in competition with their employer. These clauses require specialist advice from an advisor with experience of providing enforceable legal protection for corporate business assets.

The policy should be a combination of the following: -

1. Signed template explaining employee and management obligations regarding data protection.
2. Board's strategy based on Cyber Defences in line with company cyber insurance policy.
3. Board's written acceptance of GDPR and regulatory compliance rules.
4. Board investment in latest service or technology platform to protect against all known breaches and attacks.
5. Board to appoint relevant personnel to manage legacy change policies in line with the Cyber Security Policy.
6. Appointed personnel to report on a regular basis to the board that Cyber Defences are in line with current cyber-criminal attack surfaces and meets the cyber insurance policy and regulatory data protection requirements for up to date technology and services.

9. References

Blackburn, M. (2015, April 17). *Data Security and Breach Notification Act of 2015.* Retrieved August 19, 2016, from https://www.congress.gov/bill/114th-congress/house-bill/1770/text

ENISA. (2016, January 27). *ENISA Threat Landscape 2015.* Retrieved August 18, 2016, from https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport

ENISA. (2014, December). *Technical Guidelines on Security Measures for Article 4 and 13a*. Retrieved July 20, 2015, from http://tinyurl.com/p43dzt5

European Commission. (2016, April 11). *ePrivacy Directive: Commission launches a public consultation to kick start the review* . Retrieved August 18, 2016, from https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review

European Parliament. (2016, April 27). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. Retrieved August 18, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

UM Labs. (2014, October). *Combating Denial of Service Attacks for VoIP and UC.* Retrieved Augusr 19, 2016, from http://www.um-labs.com/SiteAssets/technical-white-papers/UC-DoSProtection.pdf