



THE CYBER RISK TOOLKIT FOR PRIVATE CLIENT PROTECTION

itcsecure.com

CONTENTS

Part 1: Who attacks and targets your clients?	P3
Part 2: Common vulnerabilities - where are your clients weak and how to manage that risk?	P5
Part 3: Why better intelligence leads to better cyber decisions?	P7
Part 4: How can your clients prevent cyber breaches?	P9
Part 5: What are the impacts of a cyber attack for your clients?	P11

WHY IS THERE A RISK:

High Net Worth (HNW) and high-profile individuals, such as actors, sports stars and media celebrities, are increasingly coming under threat from cyber risks. There are three reasons for this: they have secrets, their reputation is invaluable, and they have money. They are what an attacker calls a High Value Target (HVT). This 'toolkit' is an end-to-end advisory piece on the risks facing HNW clients and how to protect them. It provides guidance and insight into the people who want to attack private clients, common vulnerabilities, importance of cyber intelligence, steps for prevention, and the potential impacts of a cyber breach.

The cyber threat is real, but it should not be feared. It is a risk, like many others, which needs managing to mitigate the threat.

PART 1

WHO ATTACKS AND TARGETS YOUR CLIENTS?

Cyber criminals, armed with sophisticated and complex tools, are increasingly targeting HNW individuals and people of prominence. In the knowledge that these individuals' levels of cyber defence and protection differ dramatically to large scale organisations and firms, many cyber criminals pursue notoriety by striving to either leak or expose the personal/private data and information of high profile individuals.

This pursuit not only offers the criminal potential financial gain, but legitimacy and elevated status amongst their cyber criminal peers. Attacks can have grave and profound consequences for individuals when their reputation and brand has been compromised and, in some cases, irreversibly damaged. Considering what is at stake, cyber criminals refer to these lucrative marks as 'HVTs'.

In broad terms, there are four groups of attackers HNWs and high-profile individuals should be wary of:

Criminals



The most common form of attacker in the cyber space are criminals. Primarily motivated by money, these attackers typically utilise a broad range of ingenious and calculating methods to ensure a target is compromised. Gone are the days of physically targeting banks. Criminals are now able to coerce vulnerable targets from their desks using malware and ransomware to reap a financial reward.

Hacktivists



Motivated either by ideology or personal principles, hacktivists have used the cyber space to promote political ideas, support campaigns and denounce individuals. Whether it is 'Anonymous' or animal rights groups, HVTs are at risk of being used or exposed to benefit the hacktivists' cause. The resources and motives of hacktivists should not be underestimated: HVTs' private lives, family and wider privacy are all part of the target.

Uninformed



The label 'The Uninformed' usually refers to young people setting their own hacking challenges, simply for the thrill or the fun of it. Often, teenagers sat in their bedrooms display little interest or regard for the impact they inflict on their targets. Whether to cause personal intrusion, disruption, or the closure of a corporate or government entity which individuals are reliant upon, the effects have a significant impact on people's lives.

Nation States



Nation States, or nation backed hacking as it is less commonly known, poses a significant threat to some individuals. Some Nation States' intelligence agencies have been known to target HNWs or prominent individuals who have either denounced, exposed or threatened the State in question. A variety of Nation States have also been known to indirectly support hacktivists by turning a 'blind eye' when individuals deemed to be a threat to national security are targeted. Nation States typically have a wide range of powerful capabilities and resources at their disposal to target HVTs.

TO CONCLUDE

HNWs and high-profile individuals need to understand the realities and threats facing them and, in turn, take measures to mitigate these risks. They must take steps to understand who wants to attack them to protect their online activities from anyone wanting to gain illegal access.

Weaknesses in technology, but also a lack of good cyber governance and procedures amongst a HVTs wider entourage, provides potential hackers with multiple opportunities. Cyber attacks are on the rise, and the complexity with which they are being delivered is increasing. Being aware of what form an attack takes, the vulnerabilities that exist for a client and where they are exposed is essential for HVTs and their team to grasp and then rectify. Threats needn't be frightening when it comes to cyber security – it's simply about managing risk, being aware and being prepared.

PART 2

COMMON VULNERABILITIES – WHERE YOUR CLIENTS ARE WEAK AND HOW TO MANAGE THAT RISK.

High Value Targets (HVTs) are prime and lucrative targets for any would-be hacker. The threats are real and are ever increasing in both nature and complexity. Taking advantage of vulnerabilities and less sophisticated levels of cyber protection ensures High Value Targets (HVTs) are an attractive focus for the world's cyber criminal community.

Once a target has been chosen, an attacker will conduct extensive research to identify the areas of vulnerability/weakness that will enable them to compromise and penetrate private data of the target in question. Exploitation can take the form of financial gain or can even be motivated by harming the HVTs reputation and privacy. In some cases, attackers have been known to conduct three months digital research to secure upwards in excess of £500,000 in financial gains. Exploiting targets' vulnerabilities provides attackers with a comprehensive map and understanding of an HVTs life.

Cyber security is about risk management. The steps taken to protect an individual's digital life should be considered and implemented just as one would approach physical security. For example, an HVTs home may be supported with state-of-the-art security systems, but rarely is this applied to their mobile technology like home servers or any other form of connected devices - all of which provide layers of vulnerabilities.

WHAT ARE THE COMMON VULNERABILITIES?

Unfortunately, when considering cyber attacks, some individuals automatically think solely about the technological implications. Clearly, technology is important in defending against potential attacks but should not be viewed in isolation. Comprehensive deterrents in cyber security reach well beyond technological configurations and solutions. It is understanding, education and governance that ensures individuals consider cyber security as another part of risk management. Ultimately, it is how an individual manages this risk that ensures good levels of protection.

For example, 90% of successful cyber attacks involve either the HVT directly or their wider entourage or internal stakeholders. Points of weakness and lack of education/ governance in these wider circles enable would-be-attackers to use malware disguised as online adverts, banners, phishing emails or social engineering to penetrate and attack targets.

Behaviour, rather than technology, can lead to these breaches. Individuals have a responsibility to form a human firewall around a HVT. Friends, families, cleaners, chauffeurs, agents, and so on, can either be part of the problem, or part of the defence. People who are ignorant to the risks can easily be manipulated to provide access to the target.

TO CONCLUDE

A HVTs' wider team and entourage cannot be neglected in a cyber security plan. By exploiting those around the target, attackers can gain access to sensitive data that is valuable either financially or reputationally.

Addressing the threats head-on by educating not only the HVT, but their wider team, is essential in promoting good governance and the appropriate procedures. Combined with technical solutions, individuals are finally able to mitigate and manage these risks.

PART 3

WHY BETTER INTELLIGENCE LEADS TO BETTER CYBER DECISIONS?

High Net Worth (HNW) or high-profile individuals require a comprehensive understanding of their digital footprint. They need to be aware of who can see their digital presence and what information is accessible. This includes what appears on social media, Wikipedia, their company profile, the open source internet and probably most importantly, the deep and dark web.

Being aware and on top of both positive and negative content/news/information affords individuals and their wider support team the opportunity for a remediation strategy against attacks.

Digital footprints, typically conducted by third parties, provide a comprehensive map of an individual's digital trail on both the deep and dark web. Typically misunderstood, the dark web is a trading location and collection of underground communities that commonly conducts illegal and exploitative activities. Aided by anonymity and the use of cryptocurrency services, the dark web is the preferred platform for hackers to sell the illicit content of prominent individuals, such as stolen information, personal pictures, sensitive emails and financial data.

With a lack of cyber threat intelligence, high profile individuals surrender their ability to monitor and stay abreast of their own reputation. As most of the major press have a presence on the dark web, monitoring their digital footprint is vital for those looking to secure their reputation, especially as most individuals don't have the ability or knowledge to navigate or access these darknet websites.

A digital footprint is a necessary requirement that enables HNWs and prominent individuals to be one step ahead of would-be attackers. It provides valuable insight to enable individuals to take proactive steps, implement protection measures and, in some cases, remove or pacify legacy material that could be used to harm the individual's reputation.

Prominent individuals and their wider team must gain a greater understanding of the ever-increasing changes to the cyber risk landscape. Important questions such as: 'what are the latest attack methods used by hackers?'; 'What is encryption?'; 'How can I identify a phishing email?'; and 'Is WhatsApp secure?', all impact aspects of their daily lives.

Ransomware is one threat that takes a variety of forms to initiate attacks on high value targets (HVTs). For example, the likes of Apple and Microsoft continuously work on their operating systems and build specific patches for new vulnerabilities. Attackers then analyse that patch, take it apart, and pinpoint a weakness. They then create a piece of malware to specifically attack the weakness, which they mass distribute to snare parties who have yet to install that patch on their system. Therefore, it's vital to keep systems updated as soon as patches become available, and before the hackers release their attack.

TO CONCLUDE

We regularly see HNWs and high-profile individuals failing to implement their patch defences. Naively, many are not prepared to be without their mobile phone for half an hour and continually put off these updates.

Identifying what an attacker can uncover or use to their advantage early empowers confidence for HNWs to be able to operate safely.

Individuals should understand what they need to protect, how much they want to protect it, and the required steps they must take to ensure their digital profile is ultimately secure. It is a necessity that requires comprehensive support and counsel to mitigate the risks.

PART 4

HOW CAN YOUR CLIENTS PREVENT CYBER BREACHES?

'Cyber' doesn't have to be difficult to understand. Albeit complex and daunting in the first appearance, cyber security is simply a risk that needs to be managed and mitigated like any other.

HNW and high-profile individuals are particularly high-risk targets, but bespoke cyber risk solutions can be tailored in conjunction with publicists, lawyers and managers/agents.

Good risk management enables clients to eradicate vulnerabilities and significantly reduces the chance of motivated hackers breaching client data and private material.

Examples of these steps include:

- ▶ The use of strong passwords
- ▶ Updating software regularly
- ▶ Implementing and configuring the right technology
- ▶ Improving the understanding of threats, not only to the client but their wider team and stakeholders.










Strong password and patch management are typically overlooked due to their perceived simplicity or relevance; yet, these are usually the first targets of vulnerability that would-be hackers will focus on and compromise. Emails designed to cause damage, typically used by hackers, are called 'phishing emails'. These emails contain either ransomware links or malicious software that, when opened, sits in the victim's system and records keystrokes, or even worse, steals information.

EASY STEPS

Easy steps can also be taken to mitigate the risks facing mobile devices. If a HNW or high-profile individual loses a device, it's important that the device can be wiped remotely to ensure strangers aren't allowed access to its contents.

Perhaps even more importantly, training is essential for any prominent individual and their wider team. Threat prevention is firmly centred around this training. What to look for and what-not-to-do forms the basis of good cyber governance. Simple oversights such as geo-tagging on social media, downloading free apps or opening malicious links all pose threats to a client.

Frequently asked questions:

-  What is phishing?
-  How do I know if something is potentially malicious?
-  I've clicked on a link I think is malicious, what do I do now?
-  How do I use the Internet safely?
-  What is a good password?
-  What's two-factor authentication?
-  How do I stop everybody looking at my social profiles?
-  What is the Cloud?
-  Is public Wi-Fi dangerous?

TO CONCLUDE

Don't be scared of the cyber threat; rather, be aware, be proactive and be supported by experts who speak your language. Ultimately, it is the management of 'cyber risk' that empowers your clients to run their businesses and lives online with confidence.

PART 5

WHAT ARE THE IMPACTS OF A CYBER ATTACK FOR YOUR CLIENTS?

The spike in cyber attacks on HNWs and high-profile individuals is on the rise. HVTs are primarily targeted in the following areas:

Financial



HVTs commonly fall victim to financial loss through sophisticated, researched and well planned targeted attacks. The potential loss incurred is infinite, and due to hackers' use of cryptocurrency in ransomware attacks, it is rare, if not near impossible, for law enforcement to ever recover payments or losses.

Simple mistakes, such as clicking on a malicious link imbedded in an email, can quickly escalate and have significant financial implications. Breaches and leaks of personal data can also lead to attackers accessing an individual's bank details and financial assets, which in turn can have detrimental financial and reputational consequences.

Reputation



Reputational damage caused by cyber attacks can be irreversible and long-lasting. Brand, transparency and trust are all essential parts of an HVTs' makeup and if tarnished can lead to loss of sponsorship, business, standing or value. Once a reputation has been damaged, it is incredibly difficult to reassert trust and transparency.

The iCloud leaks which began in 2014 demonstrated how the leaking of private and sensitive data, in this case images, can have a detrimental effect on how the external world views the individual in question thereafter. Brand management of one's digital footprint is essential. As many are aware, 'perception is reality'.

Business sensitive information



There has also been increasing examples of how attackers have focused their attention on the corporate entities of leading and prominent business individuals. Sensitive information surrounding contract negotiations has been leaked, in some cases resulting in fluctuations in valuations or even collapses.

Private information can be used for extortion or blackmail, and damages can be far-reaching. Clients involved with the respective businesses' may become either embroiled in, or privy to, a company's private information.

Given the potential consequences, the privacy and security of private clients is imperative. Individuals need to be able to operate with confidence within the digital space, happy in the knowledge that their privacy, reputation and data is securely protected.



Why ITC

Established in 1995, ITC continues to evolve in the face of the everchanging security threat landscape. With capabilities in on-premise, cloud-based and hybrid security, ITC is a cyber consulting and managed security service provider like no other.

Including former members of British intelligence, experienced cyber security professionals and access to some of the World's leading security experts, ITC provide discreet risk advice to a number of the World's leading brands

Contact Us

If you would like to know more about our market leading security consulting services, our Netsure360° portfolio or want to hear more about our Security Insights programme; go to www.itcsecure.com, call **0207 517 3900** or email us at marketing@itcsecure.com

