FS Club
News Events Partnerships

How Insecure Are Your Websites? The Enigma of Digital Certificates (PKI)

Andrew Jenkinson, CEO, Cybersec Innovation Partners

Thursday, 06 January 2022, 15:00 GMT

A Word From Today's Chairwoman

Charlotte Dawber-Ashley

Manager, FS Club

Z/Yen Group

Platinum Sponsors

Invest Northern Ireland

CDI
CHINA DEVELOPMENT INSTITUTE
中国（深圳）综合开发研究院

FINANCE MONTRÉAL

AIFC

Seoul
Together we stand

Busan Finance Center

HK FINANCIAL SERVICES DEVELOPMENT COUNCIL
香港金融發展局

LuxembourgforFinance
Agency for the Development of the Financial Centre

ADGM
AN INTERNATIONAL FINANCIAL CENTRE

Dubai International Financial Centre

THE GOVERNMENT OF MOSCOW
The Department for External Economic and International Relations of Moscow

G T
Global Times Consulting

Gold Sponsors

Aptitude SOFTWARE

BRIDGEWORKS

FEATURE SPACE

OUTSMART RISK

ARBORETUM

Crown Agents Bank

CERIDIAN

ENTRUST

Silver Sponsors

Bottomline

GPS
global processing services

BCS CONSULTING
Expect Excellence

P2 CONSULTING

The Technium Global
SERVICE WITH INTEGRITY

expert.ai

CLOUDSOFT

PRAXITY™
Empowering Business Globally

Bronze Sponsors

Profile Software

(expleo)

CONTACT PARTNERS

alyne

ESTATES AND INFRASTRUCTURE EXCHANGE®

UDF
www.udfspace.com

Contributor Sponsors

Challenge Curve

Currencycloud

worldpay

mastercard

RADIX
THINK TANK FOR THE RADICAL CENTRE

ZB

LEI
GLOBAL LEGAL ENTITY IDENTIFIER FOUNDATION

cuffassociates
PART OF THEBES GROUP

Volanté

TRANSPARENCY TASK FORCE

CYGNETISE

Catalina Consulting

AMSOM

GIBRALTAR STOCK EXCHANGE

Today’s Agenda

15:00 – 15:05	Chairman’s Introduction
15:05 – 15:25	Keynote Presentation – Andrew Jenkinson
15:25 – 15:45	Question & Answer

Today's Speaker

Andrew Jenkinson

CEO

Cybersec Innovation Partners

CYBERSEC INNOVATION PARTNERS

WHITETHORN®

How secure are your Internet Connections and Websites

Andrew Jenkinson,
CEO

January 2022

The original code breakers

- Modern use of encryption and decryption is commonly accepted as being the use of the cipher machine Enigma. The Enigma machine was used to send and receive critical encrypted messages.

- Alan Turing developed the Bombe which decrypted the messages. Little known however, but later confirmed, the only constant element of each message was ‘Heil Hitler’. This was a major breakthrough to cracking the code.

- William Tutte then developed Collossus to decrypt the far more complex Lorenz Cipher machine.

- Turing and Tutte’s brilliant work shortened the Second World War and saved thousands of lives.

The arrival of “emails”

- With incredible acceptance and the rapid adoption of computers from the late 1930’s onwards, it was inevitable that computers would be used for digital communication.

- In 1971 Ray Tomlinson developed and sent the world’s first Electronic message (email) which sparked a communication revolution which continues to this day. Over 300 billion emails were sent every day in 2020.

The first email was Sent by computer engineer Ray Tomlinson in 1971. The email was simply a test message to himself.

The History and Emergence of PKI (Digital Passports)

- In 1976, Whitfield Diffie and Martin Hellman published a method of securely exchanging cryptographic keys over a public channel. A year later, Ron Rivest, Adi Shamir and Leonard Adleman published the first asymmetric algorithm, called RSA (Rivest-Shamir-Adleman). Several other asymmetric algorithms have been published since, and they all have one main problem. How do you prove to Bob that he is using Alice's public key and not someone else's public key?

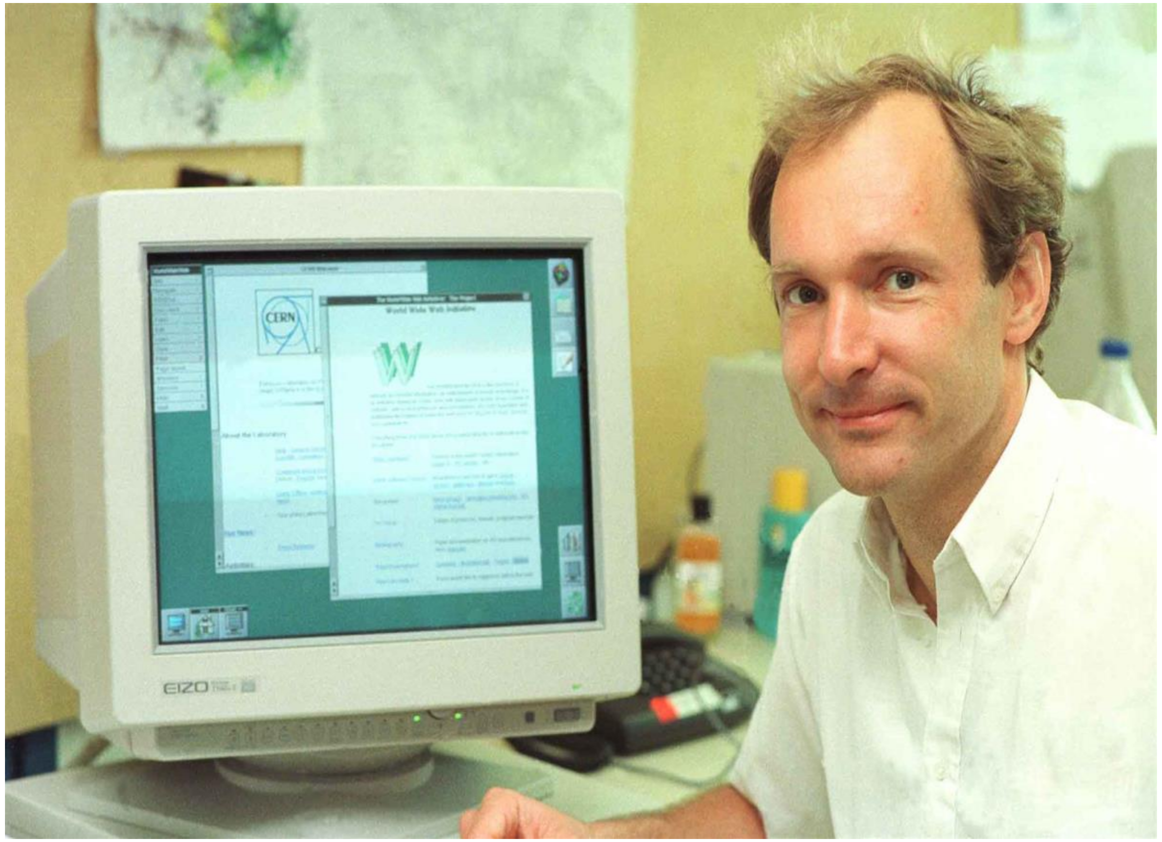
- Public Key Infrastructure (PKI) uses digital certificates and encrypted keys in a similar way to the original Enigma Machines, however, can be upgraded as required to replace or even revoke compromised certificates when and if they have been 'cracked' or deciphered. The principal of the encryption and decryption has not changed for decades. It is simply a case of having controls and management, or in the case of cyberattacks, not.

- It was not until the 1990's that PKI was globally adopted to provide encryption and decryption to the world's digital communications which became the Gold Standard.

Sadly, the PKI eco-system was pretty much compromised from the outset providing a false sense of security.

The Internet, the opportunity, and DANGER

- On August 6 1991, only 30 short years ago, Tim Berners- Lee launched the world's first ever website http://info.cern.ch This effectively fathered the World Wide Web and Internet as we know it today.
- The Digital World was about to explode, for the good.
- However, it was critical that containment and controls were adopted.
- **We are now learning the consequences of not addressing security seriously.**



Growing dependency on the internet

Computers have become an everyday way of life to the entire World, we are now totally dependent upon them.

Governments, Blue Chip organisations, Law Enforcement, Critical National Infrastructure, Telecommunication, Internet Service Providers, Digital Certificate Authorities, Central Banks, Military Forces, and everything in between have become reliant upon digital communication, all use, and are routed via the internet.

Through the formative years of the Internet and digital communication, the ability to manipulate and alter this digital information and communication was simply too irresistible for Governments and Intelligence Agencies to ensure their desired stability, control and order.

On the 11 September 2001 this changed further and very dramatically.

Exploiting PKI to monitor terrorists

Following the atrocious Terrorist attacks of 9/11 on the Twin Towers in New York, the Intelligence Community and Governments were uncompromising and relentless in their pursuit, and efforts to ensure they had full visibility and control of the Digital World.

Programmes such as PRISM, FAIRFAX and QUANTUM INSERT and hundreds more were designed, developed, deployed. And signed off costing hundreds of $billions. They were designed to intercept Terrorist communications and avoid further Terrorist attacks domestically; soon thereafter globally.

PKI was an easy technical area to manipulate and given its complexity, 'Plants' were easily hidden enabling digital interception.

HTTP (Not Secure) to HTTPS, addressing global security

- Due to the increase of cyberattacks during this period, the previously developed, but now insecure HTTP (Hypertext Transfer Protocol) security upgrading to a new, secure Protocol was discussed with the now dominant Internet Service Providers, Google, Mozilla, and others. Discussions commenced in 2013/2014 and the new, Secure version, HTTPS was mandated in 2018, its predecessor, HTTP, was deprecated.
- Google not only showed the Not Secure but also lowers the ranking of the search result for any HTTP site. This was part of the carrot and stick to encourage using more secure HTTPS. The Not Secure warning was supported and added by browser publishers.
- Paradoxically, possibly more alarmingly, a Not Secure warning in the address bar alerted Cybercriminals of security failings and ease of access. By using Open-Source Intelligence (OSINT) technology, originally developed to map one's own security facing and connected to the internet, is now being used to identify exposed, vulnerable and exploitable organisations, governments, central banks, etc.

How a monster has been turned on its creator

Red carpet is currently being laid out to any, and every cybercriminal and the criminal fraternity who now had caught up with Governments Website and Internet Offensive capabilities. What was once used to provide security, was now being used to easily identify and exploit organisations.

The Monster had been turned on its creator as confirmed in David Sangers excellent book: The Perfect Weapon.

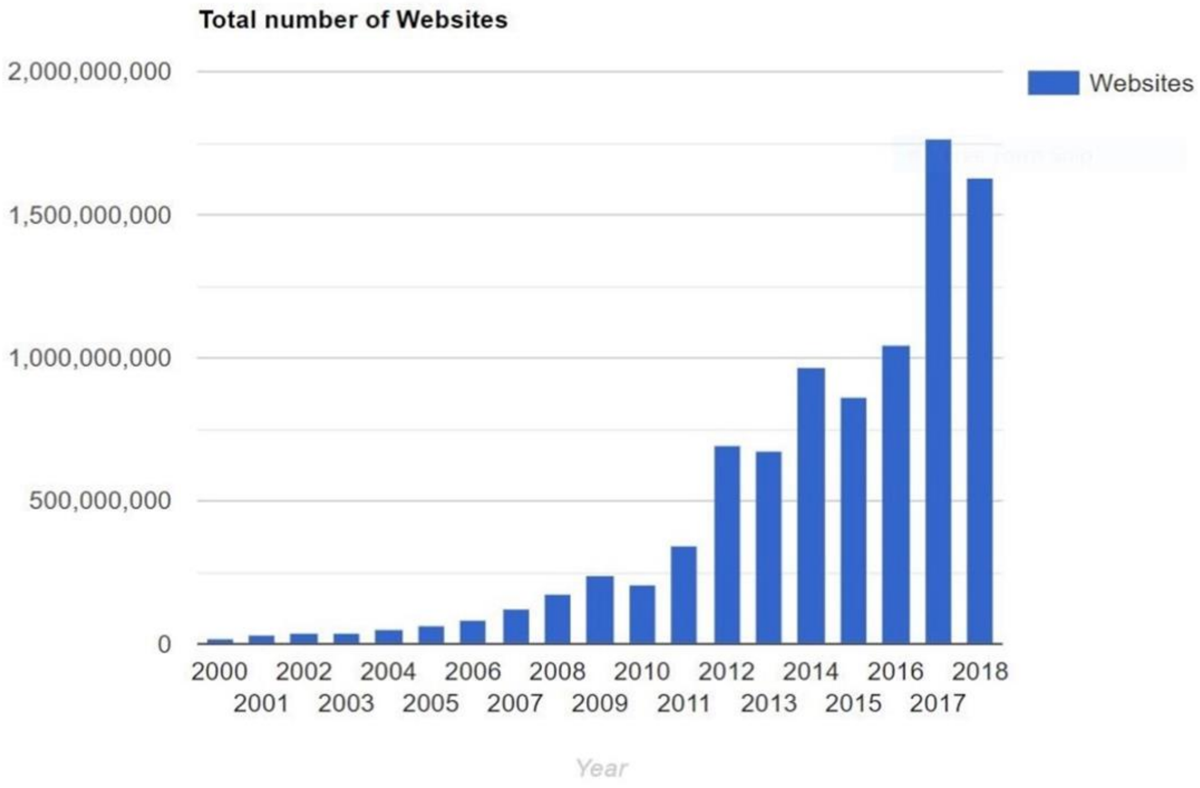
It has never been made easier for cybercriminals.

It is harder for authorities to attribute criminal activity to anything other than a region or possibly a group. Basic security oversight and dismissal of critical basic and fundamental security has facilitated more cyberattacks only increasing in scale and frequency.

There is a much better way.

FACT 1: Increasing numbers of websites

- The number of websites a company has is always miscalculated.
- Website numbers have exponentially increased over the last 20 years.
- Since the Pandemic, even more reliance upon online business has been witnessed.
- There are now some 2 billion websites.

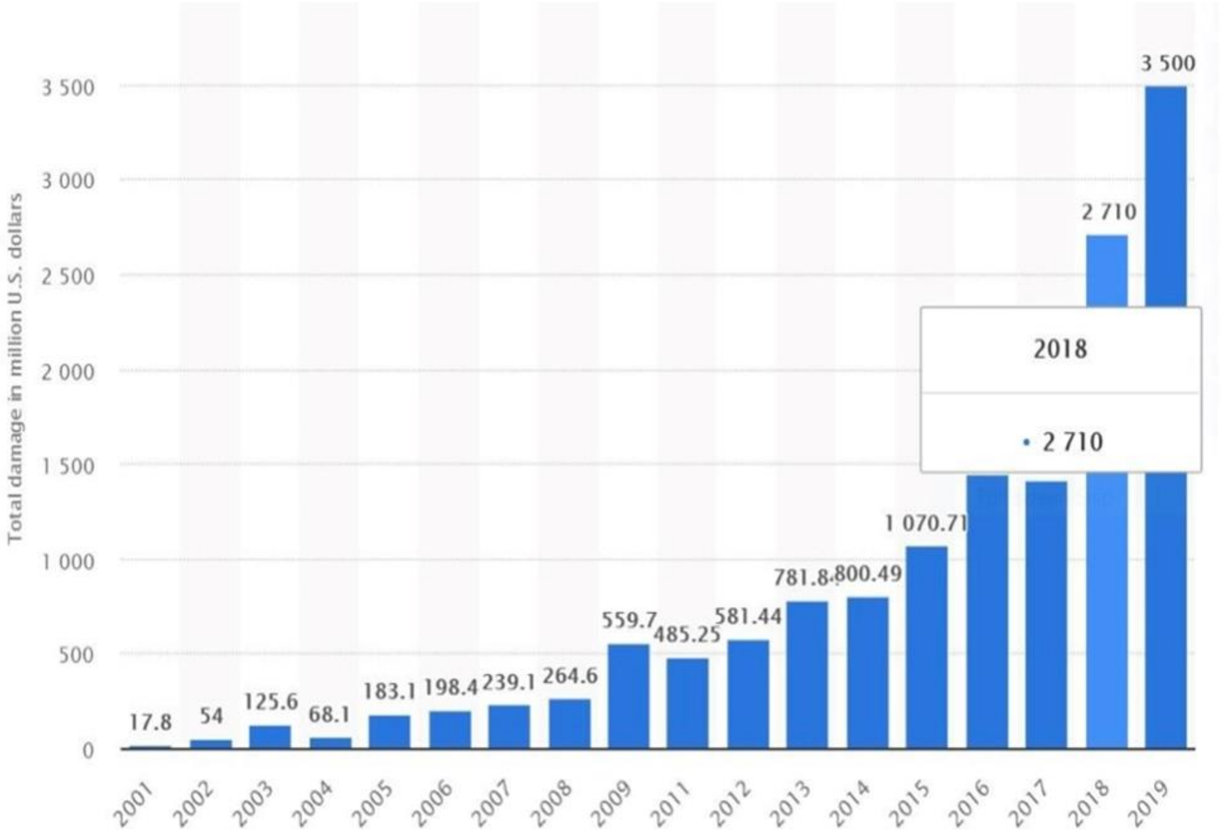


FACT 2: Increase in Cybercrime

- Numerous Global Industry experts predicted that by the end of 2021, total costs and losses to cybercrime would be $6 trillion plus.

- This made it the equivalent of the world's third largest economy by GDP. This figure is predicted to increase to $10 trillion by 2025.

- **For every $1 spent online in 2021, $2 was lost to cybercrime.**

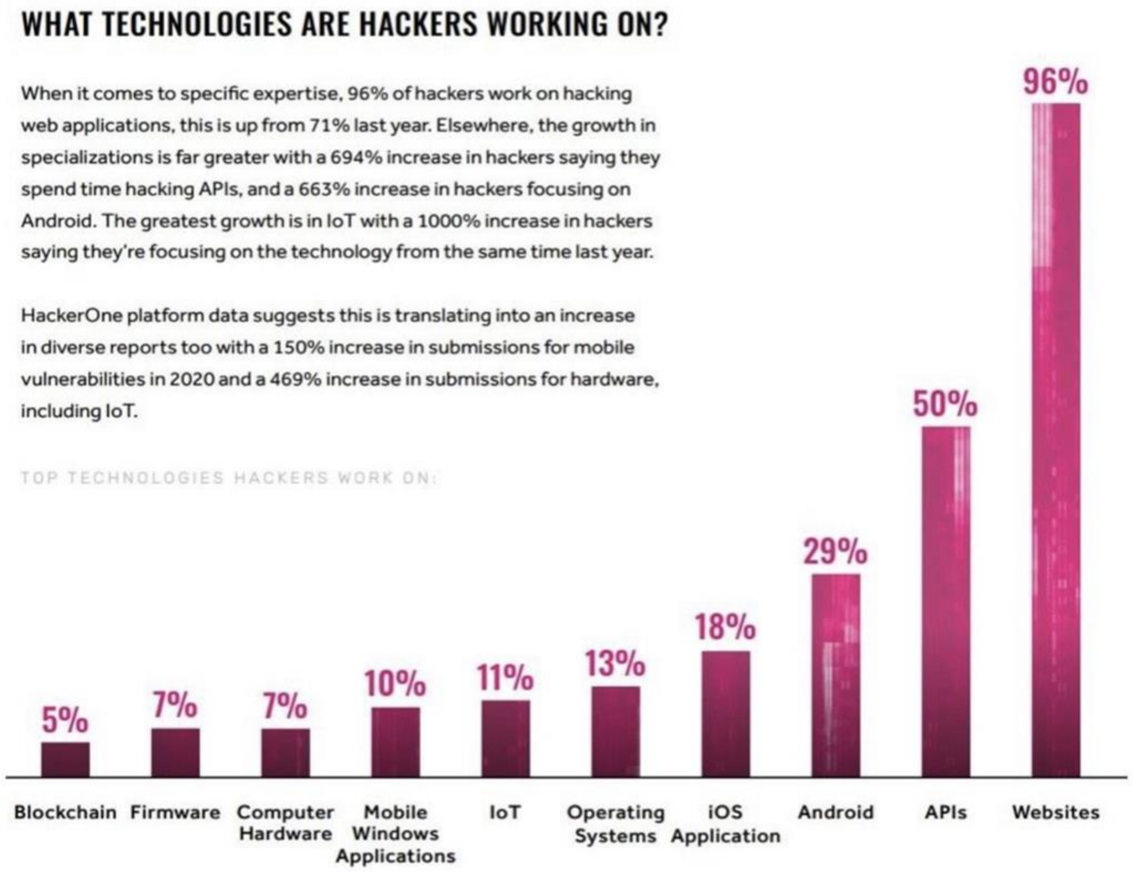


FACT 3: Hackers attack weak websites.

- In their independent 2021 Security Report, HackerOne confirmed that their research showed that 96% of Hackers hack websites, this was up from 71% in 2020.

- It is not a coincidence as CIP have researched over 1,000 companies over the last two years that have suffered cyberattacks. Our own research has found every single 'victim' maintained sub-optimal and insecure positions across their Internet facing, connected Domains and Subdomains.

- **Shut your digital doors, or you can expect hackers to enter. Once in, there is nothing to stop them.**



WHAT TECHNOLOGIES ARE HACKERS WORKING ON?

When it comes to specific expertise, 96% of hackers work on hacking web applications, this is up from 71% last year. Elsewhere, the growth in specializations is far greater with a 694% increase in hackers saying they spend time hacking APIs, and a 663% increase in hackers focusing on Android. The greatest growth is in IoT with a 1000% increase in hackers saying they're focusing on the technology from the same time last year.

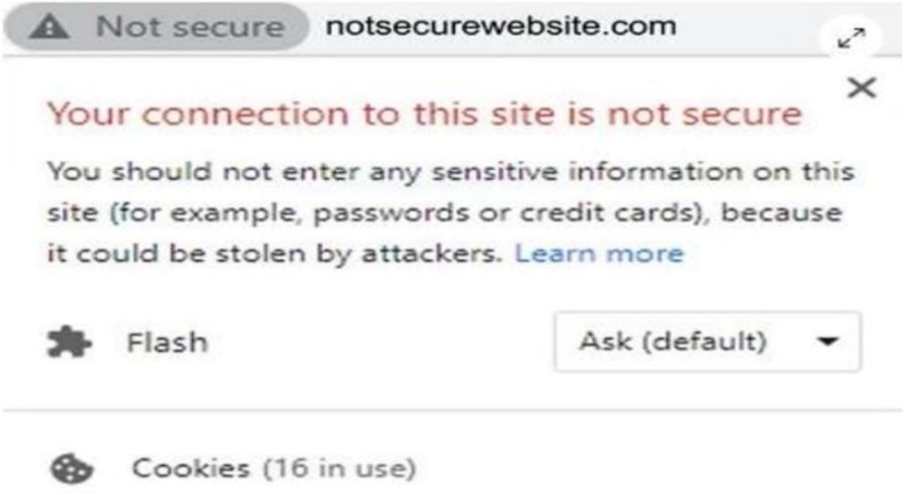
HackerOne platform data suggests this is translating into an increase in diverse reports too with a 150% increase in submissions for mobile vulnerabilities in 2020 and a 469% increase in submissions for hardware, including IoT.

TOP TECHNOLOGIES HACKERS WORK ON:

You must not ignore the warning signs

- **The Digital 'Gold Rush' to enable control and management of digital global communication, the 360-degree turn around, and retaliation of the same methods and techniques is now being used by cyber criminals. This is unequivocally destabilising our global economy and fuelling further crime.**

- Finally, I leave you with the screenshot alongside. This website is displaying the Not Secure text confirming this website is exposed and easily exploited. I will not go into detail of authentication, data integrity or lack of encryption. Suffice to say a cybercriminal finds such easily exploitable exposure irresistible and will launch cyberattacks accordingly.



Not secure notsecurewebsite.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Flash Ask (default)

Cookies (16 in use)

Not secure websites or sub domains are targeted daily – with success

- SolarWinds, the world's most prolific and damaging Cyberattack of some 18,000 company's including the US government was cyberattacked via a Not Secure subdomain - Domain Admin Access.
- Colonial Pipeline Ransomware attack via Not Secure subdomain.
- The Vatican suffered a cyberattack via one of their 82 Not Secure subdomains.
- JBS Foods suffered a cyberattack via Not Secure subdomains.
- A major UK outsourcing organisation suffered a cyberattack only weeks after we informed them and evidenced Not Secure websites.

Not secure websites or sub domains are targeted daily – with success

- Travelex floated for £billions, suffered a cyberattack via Not Secure website in Dec 2019 only months later, went into administration and sold in Dec 2020 for $1.
- CNA the global Insurance firm paid $40 million ransom after suffering a Ransomware attack via a Not Secure domain.
- SolarWinds, Colonial, The Vatican, Travelex, and CNA notified their clients, and the world, on their own websites that clearly displayed Not Secure on them.
- Kaseya Supply Chain Ransomware Attack affected hundreds of clients whilst maintaining Not Secure websites
- Blackbaud the IT provider maintained Not Secure when they were hacked, and a further 100 plus companies subsequently suffered attacks including Charities and even Bletchley Park.

There is no coincidence of the correlation between insecure websites and cyberattacks as our research and investigations have evidence on over 1,000 cyberattacked companies.

How can you stay one step ahead of the cybercriminals?

- Real time and ongoing Website & Internet Threat Analysis.
- Ensure controls and management of this critical area, not just homepages. (weakest links)
- Intellectual Property and Personal Identifiable Information are two major areas of data theft. Not Secure and Insecure websites not only facilitate their theft, but also fall foul of UKDPA and GDPR compliance laws.
- Further moves to hold Boards and Executives accountable for security oversights cannot be ignored.
- When would now be a good time to ensure perimeter security is robust and fit for purpose?

BE VIGILANT, GAIN VISIBILITY, CONTROL and SECURITY

Thank you

Contact us:

info@cybersecip.com

Cybersec Innovation Partners

24/25 The Shard

32 London Bridge Street

London SE1 9SG

Registered in England & Wales No 11465050. Registered Office: Linden House, Linden Close, Tunbridge Wells, TN4 8HH

Comments, Questions & Answers

06/01/2022

Platinum Sponsors

Invest Northern Ireland

CDI China Development Institute 中国（深圳）综合开发研究院

Finance Montréal

AIFC

Seoul Together we stand

Busan Finance Center

HK Financial Services Development Council 香港金融發展局

LuxembourgforFinance Agency for the Development of the Financial Centre

ADGM An International Financial Centre

Dubai International Financial Centre

The Government of Moscow The Department for External Economic and International Relations of Moscow

G T Global Times Consulting

Gold Sponsors

Aptitude Software

Bridgeworks

Feature Space

Outsmart Risk

Arboretum

Crown Agents Bank

Ceridian

Entrust

Silver Sponsors

Bottomline

GPS global processing services

BCS Consulting Expect Excellence

P2 Consulting

The Technium Global Service with Integrity

expert.ai

Cloudsoft

Praxity Empowering Business Globally

Bronze Sponsors

Profile Software

(expleo)

Contact Partners

alyne

Estates and Infrastructure Exchange

UDF www.udfspace.com

Contributor Sponsors

Challenge Curve

Currencycloud

worldpay

mastercard.

Radix Think Tank for the Radical Centre

ZB

LEI Global Legal Entity Identifier Foundation

cuffassociates part of Thebes Group

Volanté

Transparency Task Force

Cygnetise

Catalina Consulting

AMSOM

Gibraltar Stock Exchange

Thank You For Listening

Forthcoming Events

Tue, 11 Jan (16:00-17:00)	The New Old: Getting To Grips With Longevity
Wed, 19 Jan (11:00-11:45)	Confident, But Not Complacent
Thu, 20 Jan (11:00-11:45)	Shattering Pixels – The Metaverse & Insurance
Wed, 26 Jan (15:00-15:45)	An Update On EU Financial Services Legislation & Associated Initiatives

Visit https://fsclub.zyen.com/events/forthcoming-events/

Watch past webinars https://www.youtube.com/zyengroup