BYTES
CYBER CONSULTING

WELCOME TO

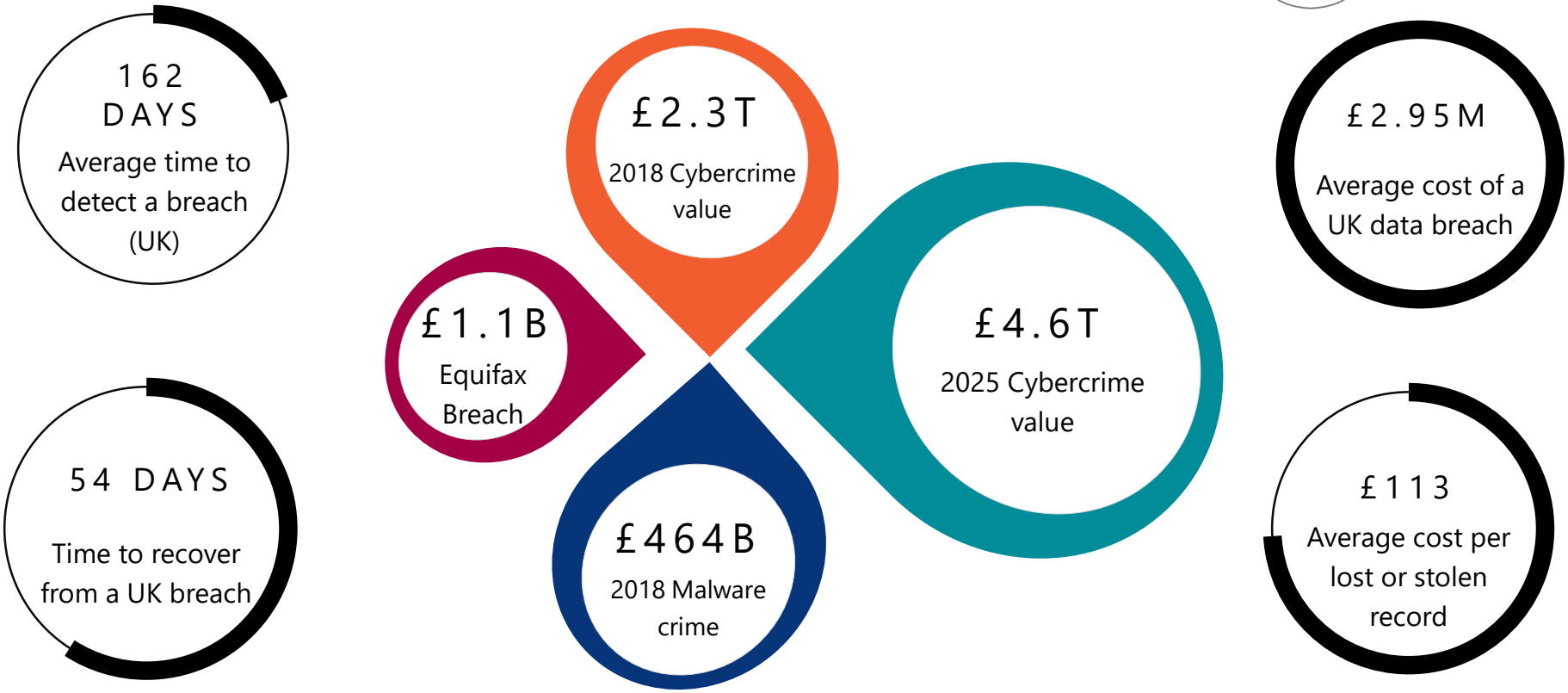
If you always do what you always did, then you always get what you always got

"The only difference between giving an infosec talk and stand-up comedy is the presence of a slide deck" - @evacide (twitter)

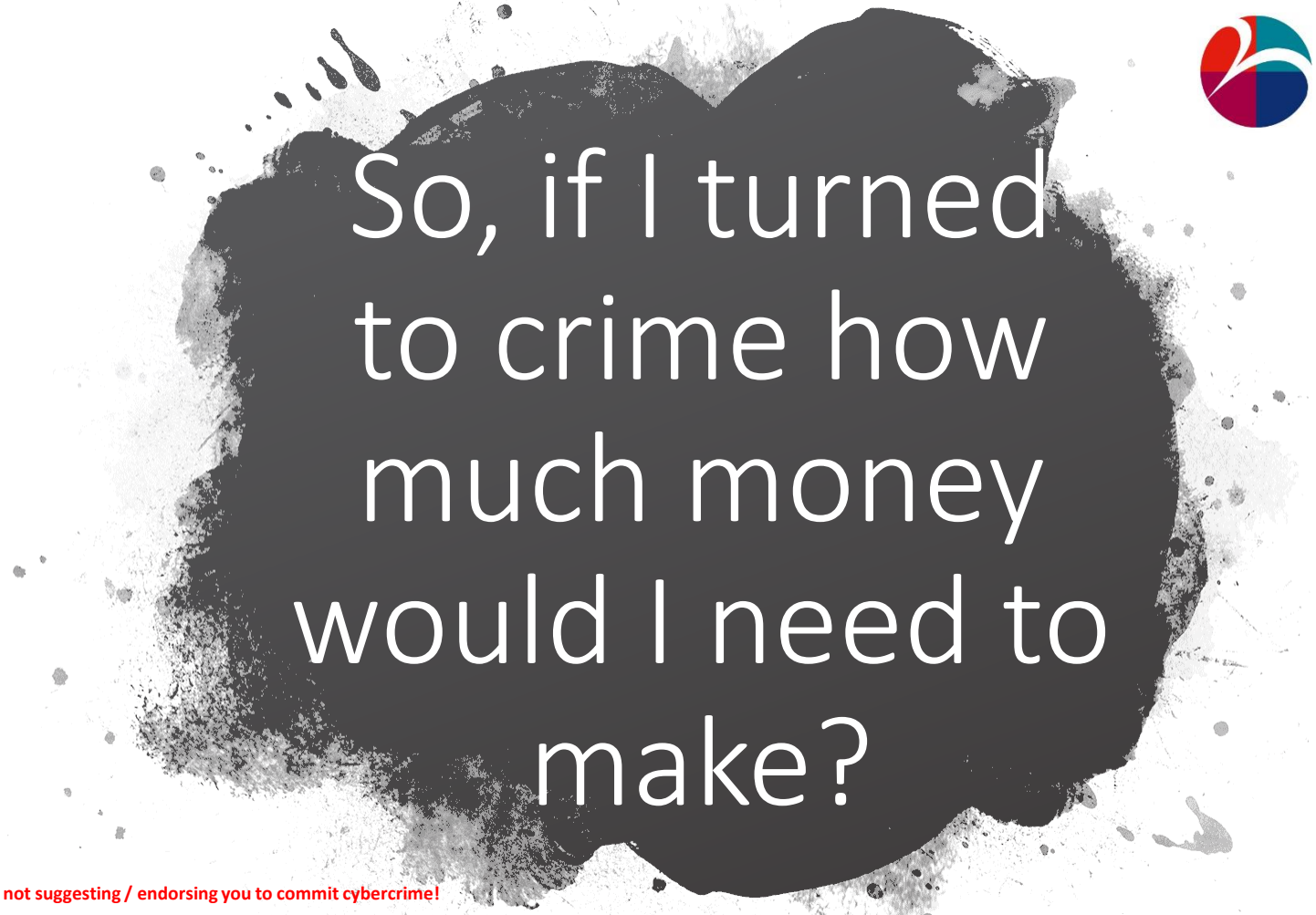
As you can tell I am not Dave Gorman

(and I don't have a checked shirt on either!)

Cybercrime stats



Stats from Ponemon Institute, IT Governance, Verizon, HP



BYTES CYBER CONSULTING

DISCLAIMER: I am not suggesting / endorsing you to commit cybercrime!

So what does crime of 2022 look like?

It depends on the technology that you use – so what are the predictions for 2022

5G will be here! (Allegedly)

- High bandwidth and low latency means Big DoS and Big DDoS!
- When private 5G is available this will be open to spoofing and jamming to interfere with normal operation
- Realtime feedback will be spoofed using man-in-the-middle attacks
- Emergency services can take down 5G networks in a crisis
- Narrow band IoT services open up new attack surfaces and opportunities

Misuse of legitimate platforms

I ordered a bag of coke

I got a bag of coke!

DISCLAIMER: This didn't really happen – but what's to say that it couldn't or isn't!

On a serious note now, what about AML?

- Misappropriation of legitimate sites is a real risk that is seen today – but by 2022 this will be extended
- Selling counterfeit, fake or illegal goods through a legitimate website means that money is also laundered in the process
- AML rules are changing globally from now until 2022
- While this is an extreme example, what happens if you accept a credit card on a website and refund the money via bank transfer?

But, AML is being assessed by machine learning

- AML is being assessed by most companies using machine learning
- Machine learning can be manipulated at multiple points (especially at data collection) – as what does normal look like anyway!
- By 2022 mainstream attacks on machine learning will affect multiple solutions (image recognition, pricing, logistics, security solutions, financial etc.)
- As the human is removed, confusion, obfuscation and deception will be used by attackers to manipulate these systems

Malware feasts on cloud deployments

- Wolters Kluwer is the latest example – suggestions of ransomware on their cloud platform
- ‘Malcrime’ growing at the rate of 300 to 450% per annum
- Emotet / Trickbot and others will surpass bitcoin mining as the risk, while cryptocurrency continues to devalue or becomes regulated
- A single class break makes millions of systems vulnerable and in the digital cold war businesses are collateral damage that cause disruption to society
- Do you have connections from the cloud back into the internal networks – and why don't you use commercial grade firewalls in the cloud rather than just the basic free one?

Internet of Everything

- New attack surfaces are present as everything can be connected (reliant on 5G)
- Suddenly this becomes about the ‘I’ and the ‘A’ and less about the ‘C’
- When this has the ability to affect life, property and wealth do we take the ‘I’ and the ‘A’ more seriously
- Everything will be able to kill you!
- What about the concepts of a digital persona (http://deadsocial.org/), digital funeral or transhumanism

How do you disable an autonomous car?

The ISF have stated that, “Digitisation promises much, and development of the next generation of technologies will bring significant benefits to business and society. To survive in the digital world organisations will have to adapt. To thrive, they must evolve”

BYTES
CYBER CONSULTING

So what lessons should we learn?

- Decommission pre-loved environments - they are an easy target
- Always build the IT layer from new to have the best advantage
- Get the basics right – as most attacks are not advanced
- Keep security solutions consistent and stable
- Monitor and understand what normal looks like
- Deal with risks and vulnerabilities as they arise – don't leave them

Alexander Graham Bell once said

"Before anything else, preparation is the key to success."

"When one door closes, another door opens; but we so often look so long and so regretfully upon the closed door, that we do not see the ones which open for us."

BYTES
CYBER CONSULTING

Well that's great – we have learned the lessons of the Cyber Criminal but what does this translate to in practical terms of me and my day job!

Threat and Risk intelligence

Understand the threat and risk landscape so that you understand what you actually face. Then you can align tech and security to fit your profile

+

Find data and cover the basics

Know where your data is and cover the basics of security (protect privileged accounts, patching, AV/AM, MFA, monitoring, DLP, web filtering) but agile

+

User & Data Centric Security

Move security to consider the real identity of the user and focus on the risk they pose to adapt the security of access and the data itself

+

Adopt the cloud but make it private

Remove pre-loved (legacy) solutions and use the cloud but adopt the latest SDWAN solutions and make the public cloud private

BYTES
CYBER CONSULTING

Questions?

Bytes can help

Cyber Consulting

- **Penetration Testing** – Crest Certified
- **Security Health Checks**
- **ISF Security Audits**
- **Virtual/ Outsourced CISO**
- **Compliance Advisory Services** - ISO, GDPR, DPA, PCI DSS
- **Red Team/Blue Team Exercises**
- **Incident Response & Breach Forensics**
- **Application Testing & Vulnerability Analysis**
- **Table Top Exercises**
- **Cyber Security Strategy/ Advisory Services**