

The information security crisis: a forensic viewpoint towards incident management

CAANZ CFO Forum - August 2019



Scott Culp
Microsoft
2000

The 10 Immutable Laws of Security.

1. If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.

Email



WEAPONS
DIRECTOR 2

W 40

791

2. If a bad guy can alter the operating system on your computer, it's not your computer anymore.



3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

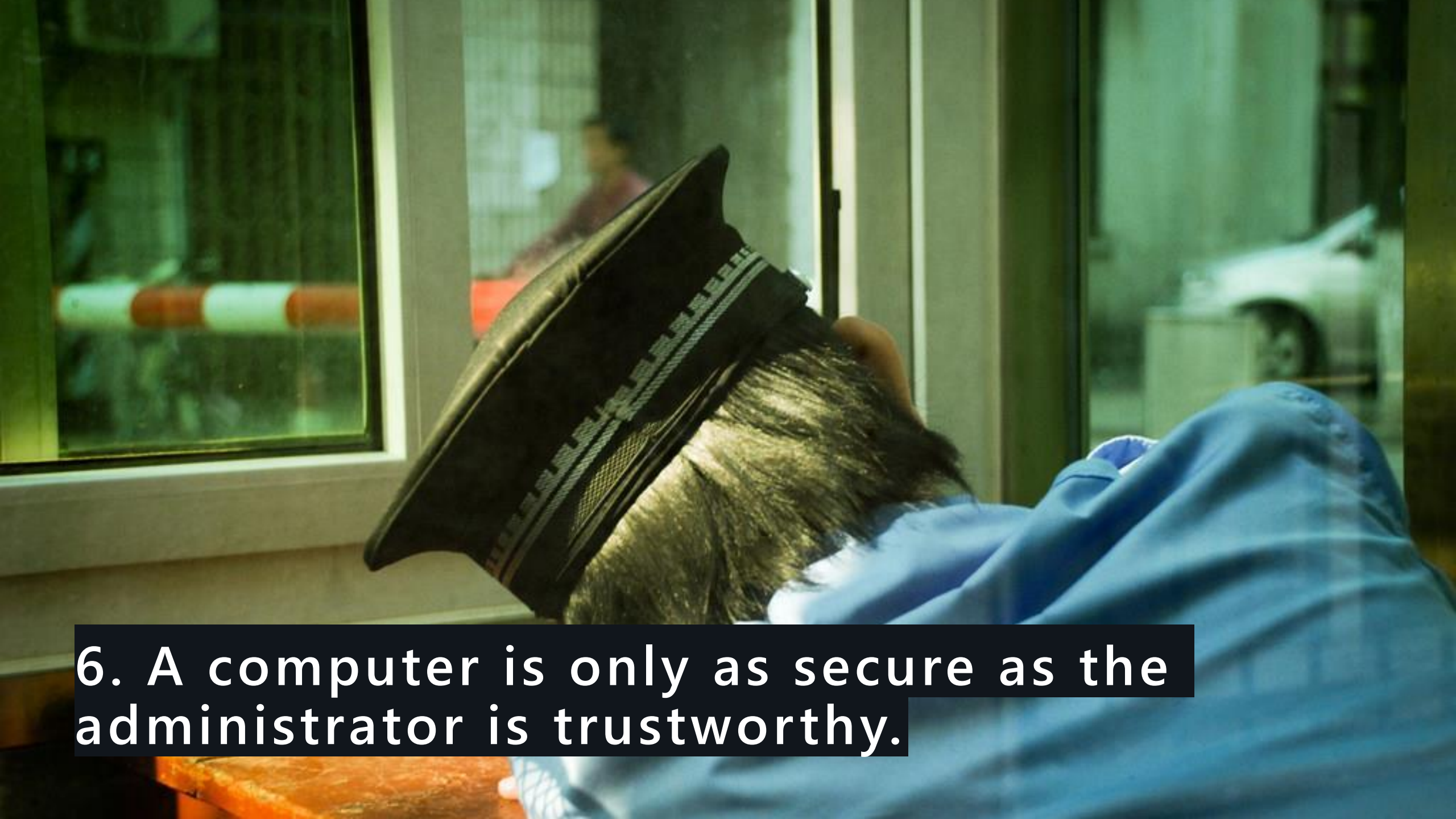
4. If you allow a bad guy to run active content in your website, it's not your website anymore.



O P E N

5. Weak passwords trump strong security.

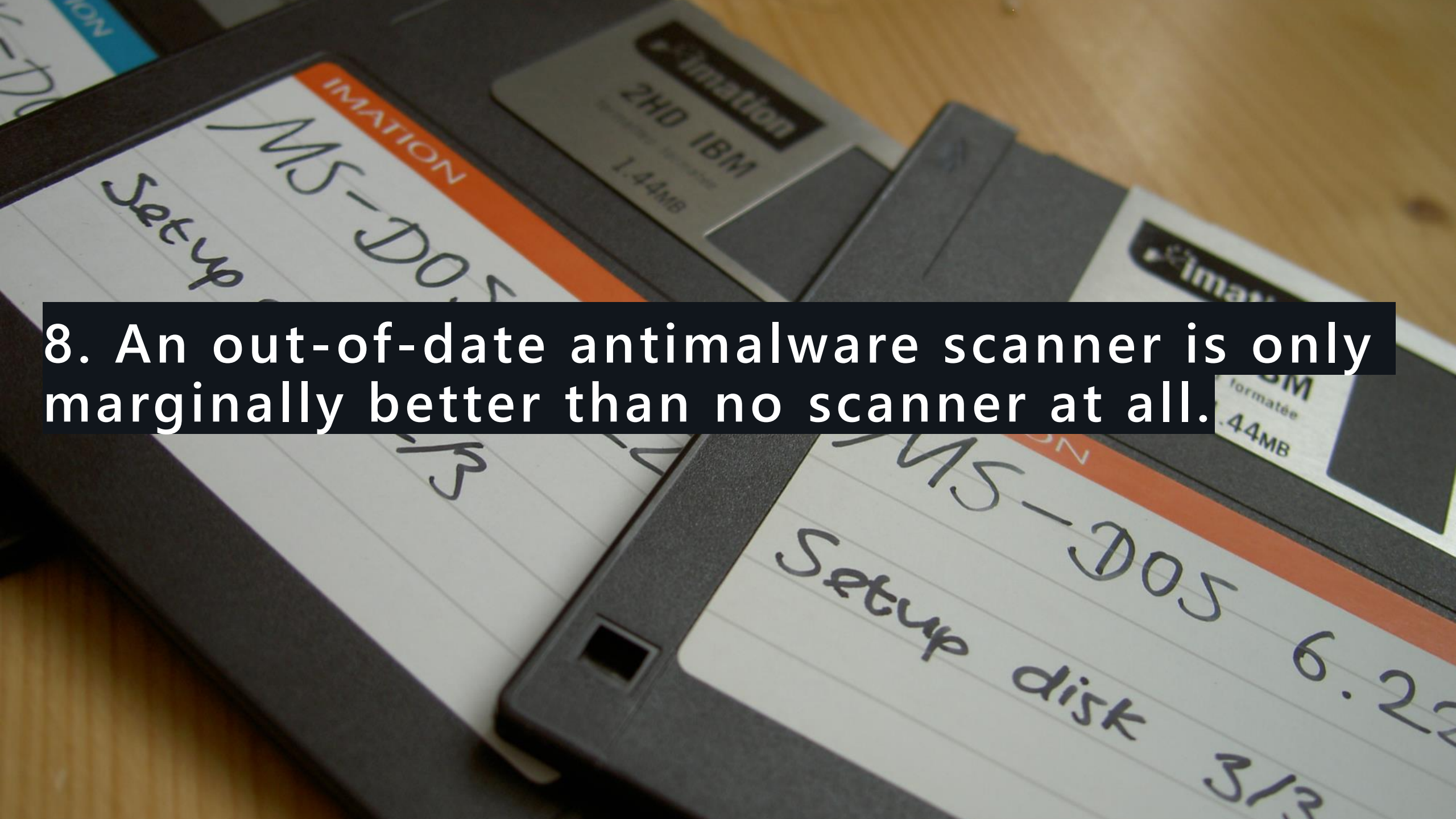
D A T A



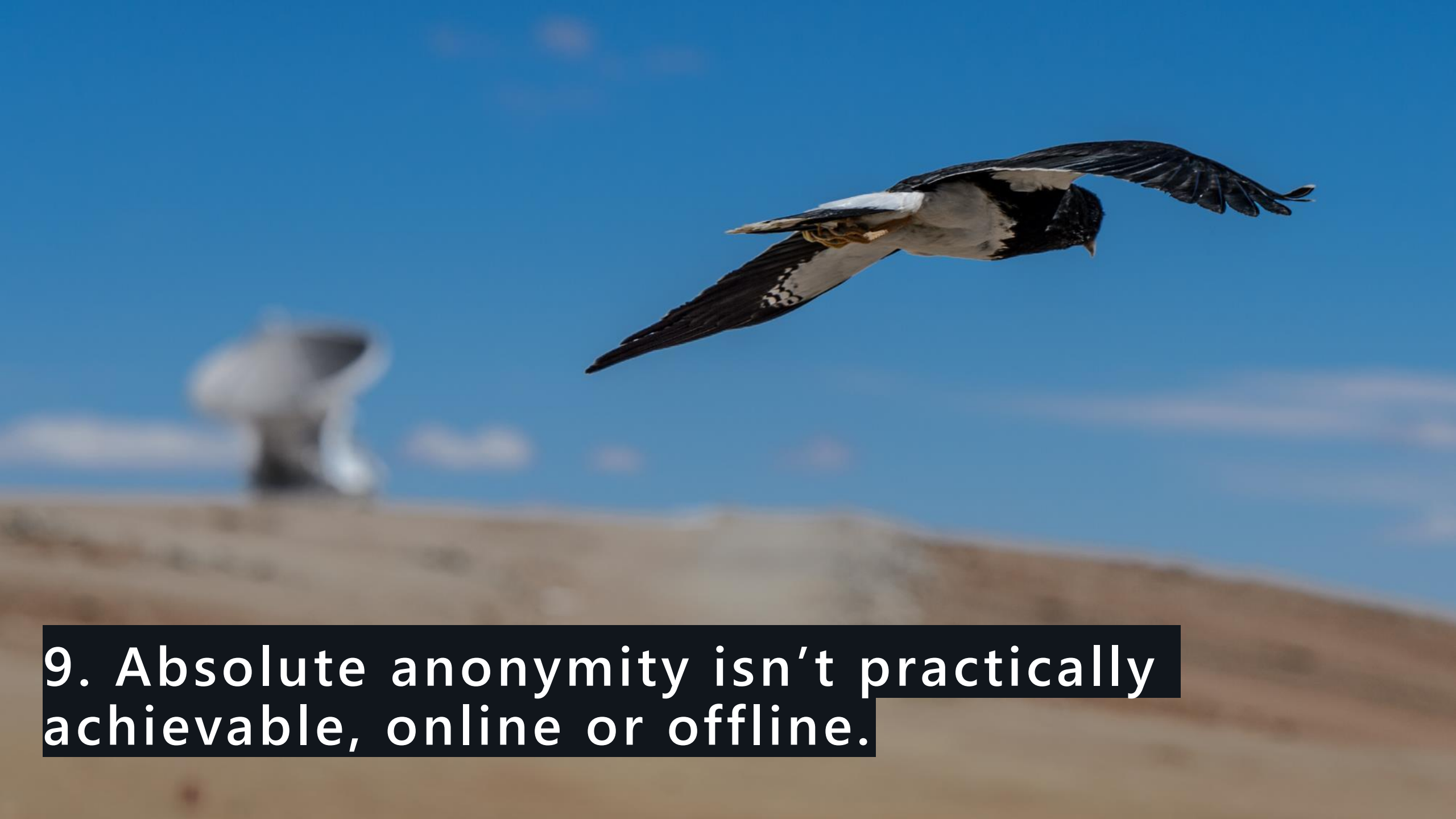
6. A computer is only as secure as the administrator is trustworthy.

7. Encrypted data is only as secure as the decryption key.





8. An out-of-date antimalware scanner is only marginally better than no scanner at all.



9. Absolute anonymity isn't practically achievable, online or offline.

10. Technology is not a panacea.



CAANZ

Cyber Incident Response for CFO's



Think Ahead



MACQUARIE
University

OPTUS



CHARTERED ACCOUNTANTS™
AUSTRALIA • NEW ZEALAND



DATE POSTED: 30/05/2019 | 3 MIN READ

Why CFOs should take the lead on cyber security

Key Findings from the CAANZ Report

- 54% were either not aware of whether their organisation had suffered an attack or thought they had not been.
- In just 8% of organisations, the CFO was responsible for the strategic direction of cyber security.
- The annual cost of cybercrime to the global economy will double from US\$3 trillion in 2015 to \$US6 trillion in 2021.
- Many organisations pinpoint cybercrime as one of their most significant threats.
- There are key reasons for the CFO to step up and play a leading role in cyber security.

1. Cybercrime is finance

- 76% were financially motivated (Verizon – 53,000).
- Damage is measured in financial terms – which the CFO quantifies and manages risk.
- The CFO has the skills and oversight to take a broader and longer-term view of the financial impact of an attack.
- The CFO looks beyond immediate issues of data loss and disturbance, to reputational/regulatory/shareholder concerns.

2. Data custodians

- The CFO is one of an organisation's key custodians of data. They increasingly assess its value and manage its lifecycle.
- They are also responsible for some of an organisation's most sensitive and valuable data, so they have an important role in identifying information that is vital to protect.

3. Highly trusted

- The CFO and the finance department are highly trusted, which can be used to promote cyber security within their organisation.
- The CFO can discuss cyber security with the board, the wider organisation and outside stakeholders. They can position it as a business and commercial risk that needs to be mitigated.
- Finance has the skills to oversee audit, inventory, testing and compliance, and will take the lead in assessing and underwriting cyber insurance.

4. In the front line of attack

- The CFO will be on the front line if cyber criminals attack. The target is most often financial data, but also the finance department and its personnel.
- After the attack, CFOs will be expected to accurately assess the damage, lead internal reactions, and communicate with stakeholders.

Cyber-resilience in FMA-regulated financial services

This report summarises the findings of our thematic review of cyber-resilience in New Zealand financial services, and provides guidance for firms in areas where we have identified the need for improvement. It will be useful for our regulated sectors, to help ensure they comply with our expectations and best practice.



Cyber Incident Response Retainer

- Panel of experts
- Support desk for ad-hoc queries
- Cyber incident response plans
- Forensic and Cyber Bulletins

<https://incidentresponse.co.nz/demos/>

Whistleblowers Service

- Independent hotline
- New Zealand experts
- 24/7 support
- Secure disclosure and reporting system

Password: *Bulletin*

Thank you

Campbell McKenzie

0800 WITNESS

021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

whistleblowers.co.nz

We help you Prepare, Respond and Recover
from **Forensic** and **Cyber** Incidents

