KryptoKloud

SECURITY MADE SIMPLE

WELCOME

Lincolnshire Care Association

KryptoCare+

COBRA Certified ✓

IASME GOVERNANCE AUDITED GOLD CERTIFIED ✓

ARMED FORCES COVENANT

GDPR CERTIFIED ✓

QUALITY PRINCIPLES CERTIFIED ✓

F-Secure

F-SECURE PLATINUM PARTNER

“The Brighter The Light, The Darker The Shadow”

- Dr Carl Jung

KryptoKloud

SECURITY MADE SIMPLE

Risky Business

10 Cyber Myths

Care Sector Risks

Lincolnshire
Care Association

KryptoKloud
Security Made Simple

Are We Good At Judging Risk?

Short Answer….

NO

Examples?

1.)

- Risk of being in a Plane Crash… 1 in 11,000,000
- Risk of being injured by your Toilet… 1 in 10,000

2.)

- Chances of winning the lottery… 1 in 45,057,474
- Chances of winning an Oscar… 1 in 11,500

3.)

- Odds of attempted house burglary in UK…1 in 100
- Odds of business cyber attack in the UK… 2 in 5

Lincolnshire
Care Association

KryptoKloud
Security Made Simple

Cognitive Bias

Optimistic Bias

It'll Be Fine!

Normalcy Bias

Well It Won't Happen To Me!

AKA The Ostrich Effect

Confirmation Bias

This Hasn't Happened to Anyone I Know

Lincolnshire
Care Association

KryptoKloud

SECURITY MADE SIMPLE

10 Cyber Security Myths that Need Busting!

Lincolnshire
Care Association

KryptoKloud
Security Made Simple

1 My Business is Too Small for a Cyber Attack

Statistics Say No

- A successful attack on SME's every 19 seconds in the UK(1)
- 4,500 a Day
- Average Costs were £25,700 for small businesses (ransom paid & hardware)
- Doesn't include loss of earnings or reputation
- 3 in 5 Small Businesses Closing within 12 months of a cyber attack
- 1 in 6 of all UK businesses fighting for survival afterwards(2)

(1) https://www.hiscoxgroup.com/news/press-releases/2018/18-10-18
(2) Hiscox Cyber Readiness Report 2021 - https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf

Lincolnshire
Care Association

KryptoKloud

Security Made Simple

2 Anti-Virus/Anti-Malware Software is Good Enough

A Question of Numbers

- Whilst a crucial first step, the odds are stack against it
- 450,000 new malwares created <u>every day</u> (1)
- 99.9% Success would still result in 164,250 that would slip through
- Anti Virus works on "signatures" so these have to be discovered before making it effective
- Would not prevent against "Zero-Day" Attacks
- Phishing attacks excluded

(1). https://www.av-test.org/en/statistics/malware/

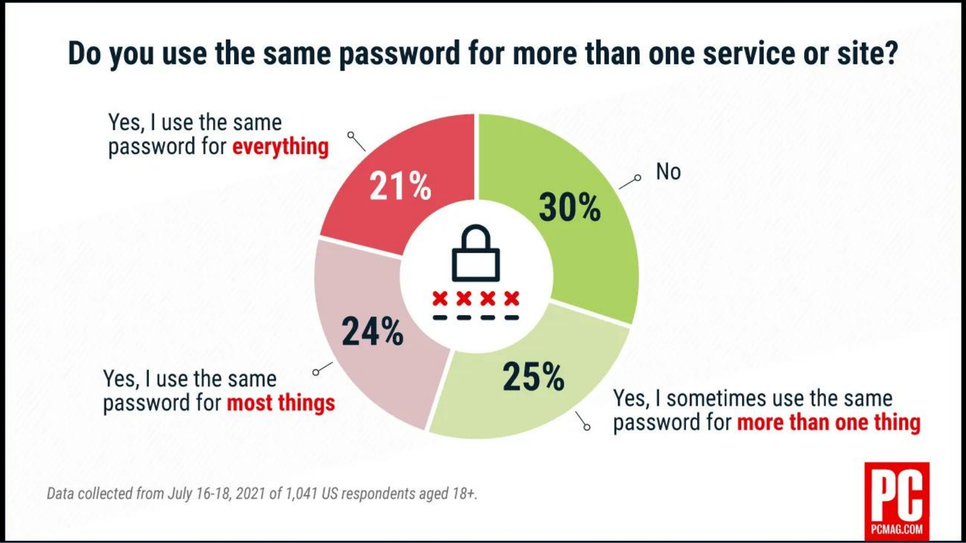
Lincolnshire Care Association

KryptoKloud
Security Made Simple

3 We Only Need Strong Passwords

Human nature is lazy

- Strong Passwords are a necessity, but repetition increases the risk of a data breach.
- Password Managers are safer
- Multi – Factor Authentication is safer still.

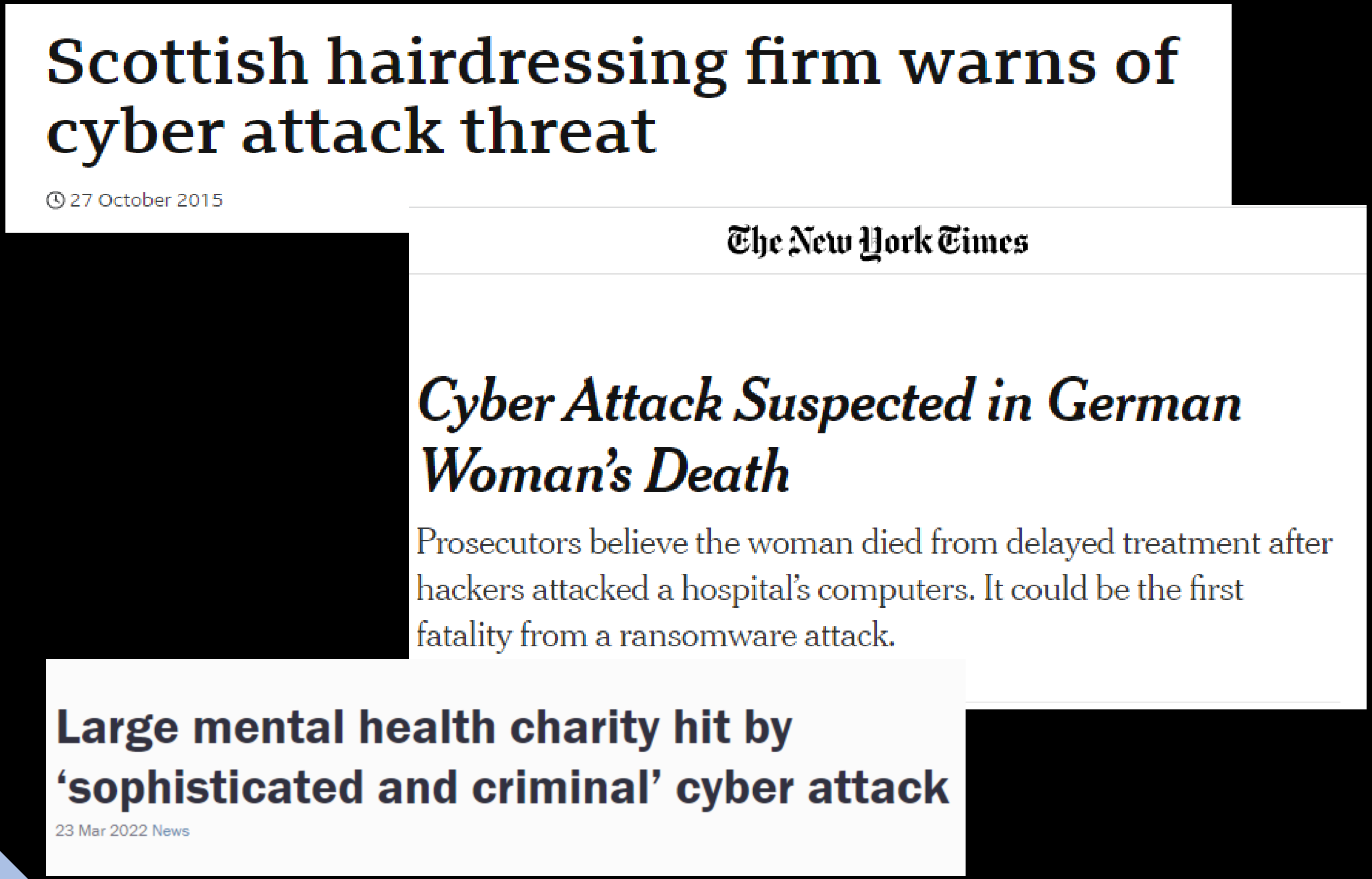


Data collected from July 16-18, 2021 of 1,041 US respondents aged 18+.

Lincolnshire Care Association

4 Our Industry Doesn't Have Any Cyber Threats

If Hairdressers, Charities and Hospitals are Attacked…



Scottish hairdressing firm warns of cyber attack threat

27 October 2015

The New York Times

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

Large mental health charity hit by 'sophisticated and criminal' cyber attack

23 Mar 2022 News

https://www.bbc.co.uk/news/uk-scotland-scotland-business-34647780
https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
https://www.civilsociety.co.uk/news/large-mental-health-charity-hit-by-sophisticated-and-criminal-cyber-attack.html

KryptoKloud
Security Made Simple

5 Bringing My Own Device is Safe

A Myth That Can Be True… Sometimes

- Examine the dangers (Laptops/Mobile Phones/Tablets)
- May be used for personal use (Websites/Downloads)
- What Wi-Fi Connections are they using? Are they secure?
- Software vulnerability patches may not be installed
- Who is using the device?
- This requires anti-malware and a strict usage, VPN and update policy
- Also requires further training for staff who engage in using their own devices.

Lincolnshire
Care Association

6 We Have Cyber Insurance, That’s Good Enough

Deal with the infection, Don’t wait to lose a limb

- Cyber Insurance is necessary, but the very act of the attack can be catastrophic.
- Cyber insurers are far more reluctant to pay out if steps have not been taken to strengthen your cyber security.
- Think about Cyber Insurance in the same manner as you would with Commercial Buildings Insurance
- Consider the reputational danger – Would you partner with an organisation you felt were a risk to your organisation’s survival?

KryptoKloud

Security Made Simple

7 Our Cyber Threats Are Only External

Its What's On the Inside That Counts

- Whilst a disgruntled employee can delete files or install malicious software, this is not the most significant risk
- Even in a team of one, there is always an internal threat.
- Ransomware attacks, cyber fraud and data theft can all be caused by "social engineering" attacks. The most common of these is Phishing.
- Even a "Good Samaritan" act can be a ploy to attack a system.

Lincolnshire Care Association

8 Our IT Team/Providers Take Care of That

Someone is Dealing With It, But Don't Ask Me How

- This is the most common response we hear at KryptoKloud
- Your own IT Team - What are they using? Anti-Virus and Firewalls?
- If they use latest generation cyber security software, how long for?
- 40 hours a week is only 24% of the time

- IT Providers – 83% of small businesses use some form
- If you're relying on them for everything, then what cyber security is being provided? Is it Anti-Virus & Firewalls?
- Are they providing 24/7 coverage?
- Almost as importantly, what's their cyber security like?

KryptoKloud
Security Made Simple

9 We Don’t Need Tests or Training

Don’t be an Ostrich

- Cyber Due Diligence also assists in providing a full awareness of where other risks may lie within an organisation.
- Cyber Awareness Training is crucial in keeping your team up to date with the risks in front of them.
- This includes awareness of Phishing, Whaling, Crabbing and Salmoning*
- This improves not only risks to your organisation but to your staff’s lives in general (Consider the time and stress of dealing with cyber fraud for an individual)

Lincolnshire
Care Association

*The last two are fake, highlighting that many employees don’t have any knowledge of technical IT terms

KryptoKloud
Security Made Simple

10 We Will See Malware Right Away

The Invisible Man

- In research by IBM, it was found that the average time that malware can be on a system without being noticed was 280 DAYS [1]
- Even more alarming a report on mid-market cyber threats found that with SME's this can shoot up to 780 DAYS [2]
- Ransomware can lay dormant on a network for weeks and months before being activated [3] .Once this occurs, research has shown that the fastest ransomware can encrypt 25,000 documents per minute [4]
- Imagine if this was in a physical context

(1) https://www.ibm.com/security/data-breach
(2) https://www.infocyte.com/resources/mid-market-threat-and-incident-response-report/
(3) https://www.newscientist.com/article/2208897-ransomware-attacks-are-on-the-rise-and-the-criminals-are-winning/
(4) https://www.splunk.com/en_us/blog/security/ransomware-encrypts-nearly-100-000-files-in-under-45-minutes.html

Lincolnshire
Care Association

KryptoKloud
Security Made Simple

10 Cyber Security Myths that Need Busting!

01 My business is too small for a cyber attack

02 Anti-Virus/Anti-Malware software is good enough

03 We only need strong passwords

04 Our industry doesn't have any cyber threats

05 Bringing my own device is safe

06 We have Cyber Insurance, that's good enough

07 Our cyber threats are only external

08 Our IT Team/Providers take care of that

09 We don't need tests or training

10 We will see malware right away

Lincolnshire
Care Association

KryptoKloud
Security Made Simple

Why Would Cyber Criminals Attack a Care Home?

- Patient care records are more valuable than credit card details on the black market ($250 compared to $5.40)
- Why? Almost a complete profile of a person's identifiable information
- Imagine if you were able to steal both from the same place…

Lincolnshire
Care Association

How Worried Should You Be?

- 67% of UK healthcare organisations suffered a cyber incident in the last year
- From March-June 2020, NHS received 41,624 malicious emails
- In the last year, over 1000 malicious emails were sent from NHS email addresses
- Health care is the only industry globally where employees are the biggest cause of data breaches:

48% Viruses or malware from third party devices including USB sticks

37% Users not following protocols or data protection policies

39% Employees sharing information with unauthorised recipients

28% Clicking on malicious links on emails and social media

KryptoKloud
Security Made Simple

Social Care Data Demands Are Changing

The Health & Care Act 2022

- The Integrated Care System (ICS) Digital Framework will change the Care sector's data accessibility and responsibility
- Further integration may mean that it is compulsory to have healthcare data shared throughout all aspects of the NHS & private healthcare sector.
- To reduce the risk of bribery within the healthcare sector, all care facilities are required to produce payment records from manufacturers and suppliers to the Secretary of State
- Failure to produce these details upon request will result in fines as of the 1st July 2022

Lincolnshire
Care Association

KryptoKloud
Security Made Simple

The NHS Data Security Protection Toolkit (DSPT)

DSPT - Designed to provide assurance that users are practising **good data security**, and personal **information is correctly handled**.

But:

- It is not always accurately completed
- It seen as a regulatory burden rather than a springboard for better, safer, digital activity
- Toolkit completion is completed as a one-off
- No questions in the toolkit about two of the areas of greatest risk identified: backups and passwords.

Beware:

- The DSPT and Cyber Essentials do not provide reassurance that your organisation is safe and protected from cyber threats.

Lincolnshire
Care Association

A Very Recent Supply Chain Attack

apetito

25th & 26th June 2022

- Apetito were the victims of a major cyber attack
- Significantly disrupted both their IT Systems and their Operations
- Unable to make any deliveries
- Unable to accept any orders at this time
- Still attempting to discover if Personally Identifiable Information has been stolen

KryptoKloud
Security Made Simple

An Even More Recent Attack on the NHS

4th August 2022

- Advanced Software became the latest NHS Supplier to be struck
- Caused all digital 111 Services to be backlogged & requiring pen and paper documentation
- Paperwork is still being run through pen & paper
- Some services may never recover
- Department of Health & Social Care are currently running enquiries into the breach and supply chain security

Lincolnshire
Care Association

KryptoKloud

SECURITY MADE SIMPLE

WHAT ARE THE SOLUTIONS?

TO BE CONTINUED…

Lincolnshire Care Association

KryptoCare+

KryptoKloud

SECURITY MADE SIMPLE

THANK YOU FOR YOUR TIME

RICHARD.MORRIS@KRYPTOKLOUD.COM
01522437123

Lincolnshire
Care Association

KryptoCare+

COBRA Certified ✓ IASME GOVERNANCE AUDITED GOLD CERTIFIED ✓ ARMED FORCES COVENANT GDPR CERTIFIED ✓ QUALITY PRINCIPLES CERTIFIED ✓ F-Secure F-SECURE PLATINUM PARTNER