

De-mystifying Multi-Factor Authentication (MFA)

Introduction: Neil Hare-Brown

- Founder: STORM Guidance: niche independent cyber advisory
- Information Security & Digital Investigator for 30 years: Financial Services, Government/Law Enforcement, Military, Industry, Retail, Marine
- Alumni Royal Holloway: MSc. Information Security
- Specialisms:
 - Cyber Risk: Assessments & Audits, Cyber Essentials
 - Cyber Incident Response: Digital & Fraud Investigations and Cyber Crisis Mgmt.
 - Cyber Insurance: Worked with cyber insurers & brokers exclusively for 8 years
- Current Assignments: 100's of Cyber & Fraud Investigations, Rapid Risk Reviews, IR Plans, Cyber|Decider & Cyber.Care in Africa



STORMGuidance

Full service offering for
reinsurers, insurers,
brokers and clients

Assess

Lightweight cyber risk assessments to enable clients to learn and improve their cyber security and to enable insurers and reinsurers to manage book risk.

Plan

Helping insured clients to create, learn (through training) and exercise/test their plans in dealing with different types of cyber incidents in the context of their business.

Respond

Delivering a fully coordinated and Integrated Cyber Incident Response Team (ReSecure & CyberCare).

Cybercrime Landscape

A Growing Risk

Cybercrime is now the fastest growing crime in the world

- 86% of breaches were financially motivated and 10% were motivated by espionage¹
- Q3 2020, saw a 50% increase in the daily average of ransomware attacks, compared to the first half of the year.²
- Ransomware and Business Email Compromise make up the majority of attacks
- Ransomware attacks in 2021 rose by 151%.²
- The amount of money pilfered in email scams in all their forms has been rising as much as 300%.³
- Data breaches increasingly feature exposing victims to significant reputational harm
- Cybercrime now costs more per year than all natural disasters

1 - Verizon

2- ThreatPost

3- Information Age Magazine



Attackers Call Centre Operation

Cybercrime Landscape

Overview of the most concerning attacks

- Attacks on national infrastructure
 - 54% of the 500 US critical infrastructure suppliers reported attempts to control systems, while 40% had experienced attempts to shut down systems
- Infiltration into supply chain (SolarWinds/Sunburst)
- BEC attacks continue to rise
 - The average cost of a wire transfer via a BEC attack, rose from \$54,000 in Q1/2020 to \$80,183 in Q2/2020
- Ransomware attacks are more sophisticated
 - A Ransomware attack every 11 seconds with average 21 days downtime
 - Over 70% are due to insecure Remote Access services
- Much more targeting of potential victim organisations
 - Many are 'leaking' data useful to attackers and are vulnerable to attack



Passwords are Useless

Engendering a false sense of security

- No defence lasts
 - “Even the finest sword plunged into salt water will eventually rust” Sun Tzu
- Passwords alone are no longer sufficient to protect personal or business accounts
 - Brute force & password spraying attacks
 - Breached data sets
 - User practice of using same password for all accounts
- Even strong passwords are vulnerable to all of the above
- We have run out of different password management strategies and can no longer consider an account with only username and password as secure
- Many services have no moved online meaning that businesses can no longer rely on the physical security and logical security of their own systems
- Online systems are mostly easily available to international attackers
- Some online service providers do not provide MFA and very few make it default

Key Cyber Safeguards

Addressing Business Email Compromise (BEC)

Implement Multi-Factor Authentication (MFA) on all online accounts.

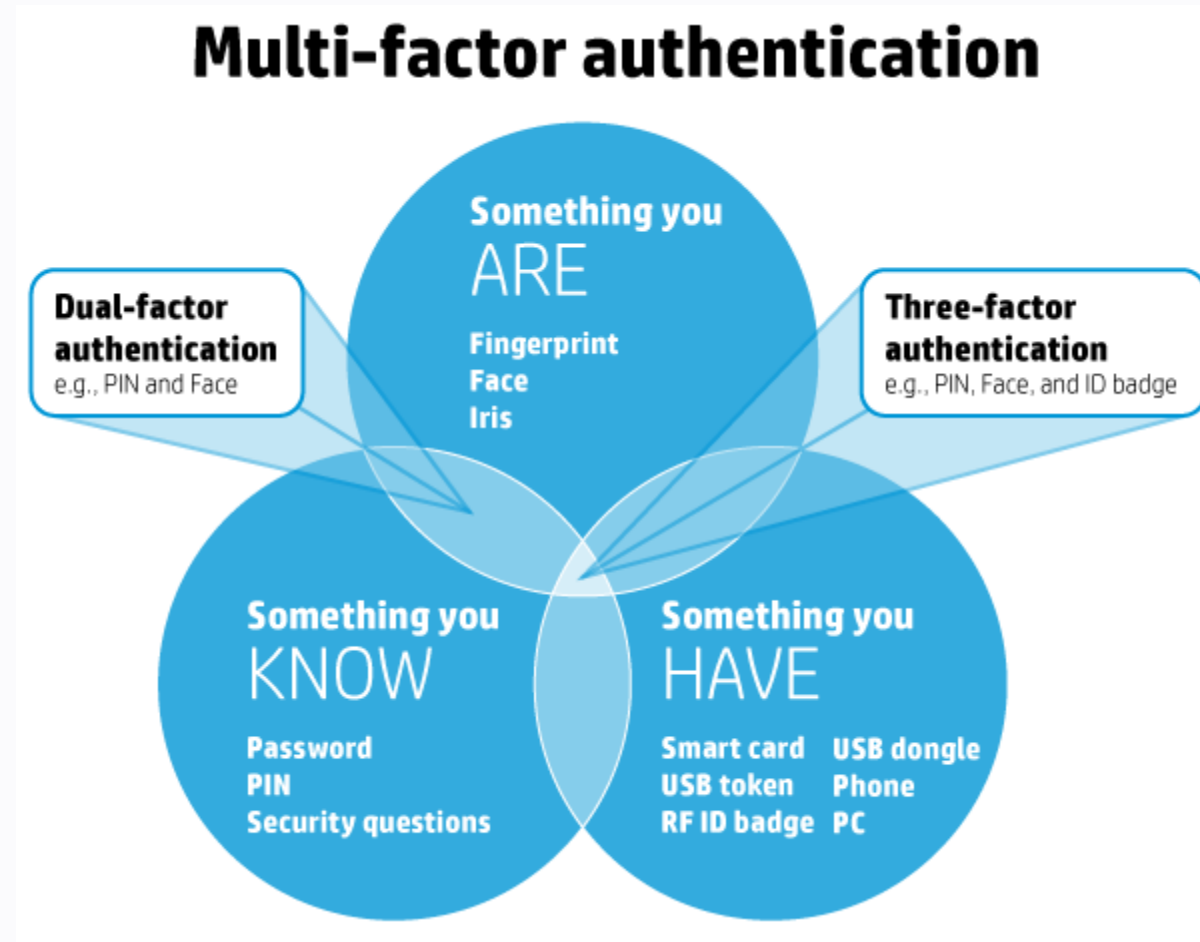
Ensure your email filters are also protected. Enact Phishing tests.

Addressing Ransomware

Ensure data backups are held offline. Segment your network and strictly control administrative user accounts. Lock down your Remote Access with MFA.

What is MFA?

Also known as Two-Factor Authentication (2FA)



Most Well-Known MFA Devices



Q: Would you be happy if your account was only protected by a password?

Criminals know that many financial transactions are arranged using accounts that are only protected by a password e.g. email

We need to apply the same protection we use for our bank account to every other online accessible account

Options for MFA code generation



- Registration of phone number. Provider sends One Time Code as SMS
- Install Authenticator App which generates One Time Code every minute.

Home / Profile / Two-Step Verification

Two-Step Verification

You are authenticated to make security changes for your account.

Time-Based One-Time Passwords (TOTP)

Step 1. Scan your QR code with a two-step verification app like Google Authenticator. (see other app options)

Step 2. Please enter the token your app is displaying.
This lets us make sure everything is set up properly.

ZOHO

One account. Access all services.

Sign In to access Mail

Email / Phone

Password

Keep me signed in [Forgot Password?](#)

Sign In

OR

[Sign in with Google or other IDPs](#)

Don't have a Zoho account? [Sign Up Now](#)

Authenticator

752203
outlook.com


Microsoft
227872
microsoft.com

Facebook
130085
edboff

Google
150451
edboff@gmail.com

2fa.directory

About Region



2FA Directory

List of websites and whether or not they support 2FA.

Backup and Sync Banking Betting Cloud Computing Communication

Creativity Crowdfunding Cryptocurrencies Developer Domains

File Management Email Video Finance Food

Key Points

- Passwords are useless! MFA needs to become ubiquitous
 - Businesses need to require MFA to be used everywhere
 - Users encouraged to enable MFA on their personal accounts
- MFA must become a 'procurement' choice
- Cloud providers need to be held to account
 - It takes hardly any development effort to implement MFA
- Use MFA:
 - From inside out - user access to all cloud apps
 - From outside-in - remote access to business network
- Authenticator apps are preferred to SMS
- Trusted devices allow for MFA code prompting to be relatively rare (even once every 90 days)




STORMGuidance
Thank you

contact@stormguidance.com

Supporting Information

www.stormguidance.com/insights


Response Investigation Consulting **STORM**Guidance Services Insights Contact



Rosie Hayes
6 days ago

How to determine the financial exposure and limits of cover needed...


With standalone cyber policies the new norm, brokers are experiencing the pressures of...



Rosie Hayes
Jan 6

The Catastrophic Effect of Cyber Incidents and 'Black Swan' Theory


Cybersecurity is one of the most glaring challenges faced by companies and government...



Rosie Hayes
Dec 17, 2020

The SUNBURST Attack – Biggest Hack for Years


Insurers to set aside funds for claims as systemic risk looks more likely Many of us have already...



Rosie Hayes
Dec 3, 2020

Calls to Close Cyber Coverage Gaps as Ransomware Payment...


There is no denying the impact COVID-19 has had on the security posture of small and medium...



Rosie Hayes
Nov 26, 2020

A Brokers' Role in Cyber Risk Management

UK insurance brokers increasingly face a more complicated role in the assessing of business cyber...



Rosie Hayes
Nov 11, 2020

The Anatomy of an Email Compromise

Business Email Compromise (BEC) is one of the more frequent forms of cybercrime today, with the...