Cybersecurity for Regulated Firms

27th January 2023

Cybersecurity for Regulated Firms – Q&A

Paul Burke, Link Group

Sam Glynn, Code In Motion

Introduction – Paul Burke FCCA

- Vice Chair of the Irish Funds FinTech Working Group
- PCF -34 Head of Accounting (Valuations) for Link Group
- Host for 1st FinTech Speaker Series event for 2023
- January is a time to reflect and ponder the year ahead

"The time to repair the roof is when the sun is shining" JFK

Intro: Knowing Me

Who? Sam Glynn, Code in Motion Ltd

What? **Independent** advisor to help you keep the cyber attackers and regulators from your door.

How? I independently **assess** your current defences using appropriate benchmarks / baselines, and then **guide** you on how to close the gaps.

Why? I know the regulated world. 10+ years advising FS firms, after 15 years with BIAM (once Ireland's largest investment manager) and BOI.

- Certified Information Security Manager (ISACA CISM)
- Certified Data Protection Officer (Compliance Institute CDPO / IAPP CIPPE & CIPM)

Intro: Knowing You

This audience has at least 3 groups:

1. Global regulated entities with access to skilled cybersecurity teams.
2. Smaller regulated entities with a reliance on external IT & security service providers.
3. FinTechs and others selling into regulated firms.

Whistle-Stop Tour
There's something for everyone in the audience

Today's Agenda

1. The Past: Central Bank Expectations
    1. 2016 Guidance
    2. 2020 Dear CEO
    3. 2021 Operational Resilience and Outsourcing
2. The Present: How Do Attackers Succeed?
    1. How are attacks succeeding?
    2. How should you be defending yourself?
3. The Future: What's on the Horizon?
    1. Introducing 'DORA The Enforcer'

The Past: Central Bank Guidance

September 2016: CIG on Cybersecurity

Cybersecurity Guidance [September 2016], split across 4 pillars:

1. IT **Risk** Oversight & Governance
2. IT **Risk** Management
3. Cybersecurity **Risk**
4. Outsourcing **Risk**

RISK is mentioned in each of the four pillars.

March 2020: Dear CEO - Asset Managers

Dear CEO issued to Asset Management firms [March 2020], including:

1. The Board does not know or care
2. The Board is not told
3. The firm can't secure what it doesn't know
4. Cybersecurity incident response plans are weak

Very specific on the minimum baseline that is now expected

December 2021: CIG on Operational Resilience

Expectations include:

1. Guideline 7**:** Identify your critical and important business services, and the technology that these rely on

2. Guideline 8**:** Identifying your 3rd party dependencies, including outsourced IT / SaaS services.

3. Guideline 9: Cyber Resilience strategies that meet operational resilience needs.

December 2021: CIG on Outsourcing

Expectations include:

1. Consideration of the cyber risk of any outsourcing, including use of the cloud - 5(c)(viii)

2. Appropriate due diligence of the Outsourced Service Provider's cybersecurity controls - 6(j)

3. Appropriate contractual clauses defining cybersecurity requirements - 7.1(h) – and right to review / test their security - 7.1(i)

You can outsource responsibility.
But you remain accountable.

The Present: Common Gaps

Perception vs Reality

“We were the victims of a sophisticated attack”

Most cyber attacks are not sophisticated.

They don’t need to be.

You might be at risk of an unsophisticated attack..

irish funds

.. If any of the following is true*:

1. Staff can download and install a new application onto their work laptop.
2. Staff can log in to a corporate system with just a password.
3. Staff can log in to a corporate system from a personal laptop.
4. You're a senior manager and you've never been involved in incident response planning or an incident simulation test.
5. You're a board member and the specific details shared about the health of your cyber defences could fit on the back of a napkin.

** MIGHT BE: You may have other security defences to mitigate the risks.*

If you're going to be a victim..

.. Don't be the victim of an unsophisticated attack:

Some simple defences include:

1. Requiring more than just a password to log in
2. Training and testing your staff regularly
3. Blocking emails that contain unusual file attachments
4. Blocking access to known malicious sites
5. Restricting the use of 'privileged accounts' (e.g., local admin accounts)
6. Disabling / Removing accounts when they are no longer needed.
7. Ensuring devices are kept up to date with the latest security updates

How to get started?

This is a road trip.

Don’t focus on identifying your preferred destination.

Focus first on identifying where you are right now.

If it’s not the safest place in town:
Start driving.

How to get started?

1. **FIRST**.. Assess where you are right now and focus on tactical improvements to secure your foundations.

2. **SECOND**.. use regulatory guidance as a baseline AND a recognized cybersecurity framework as a benchmark.

3. **AND**.. Assess and manage your outsourcing risk.

Report meaningful information to the Board:
They will be held accountable if this goes wrong.

How to prove you're in good shape?

Take the TIBER-IE Challenge!

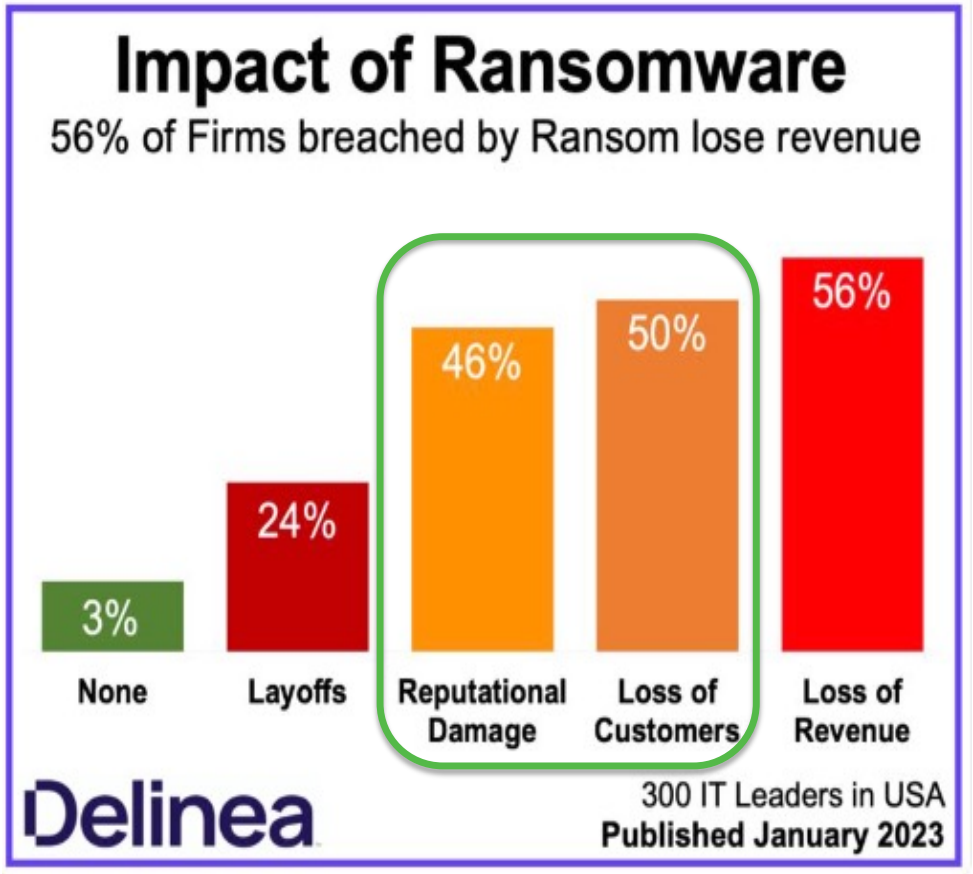
- **T**hreat Intelligence-**b**ased **E**thical **R**ed Teaming penetration test.
- European-led initiative and now promoted by Central Bank.
- Highly-skilled experts try to break into your systems.

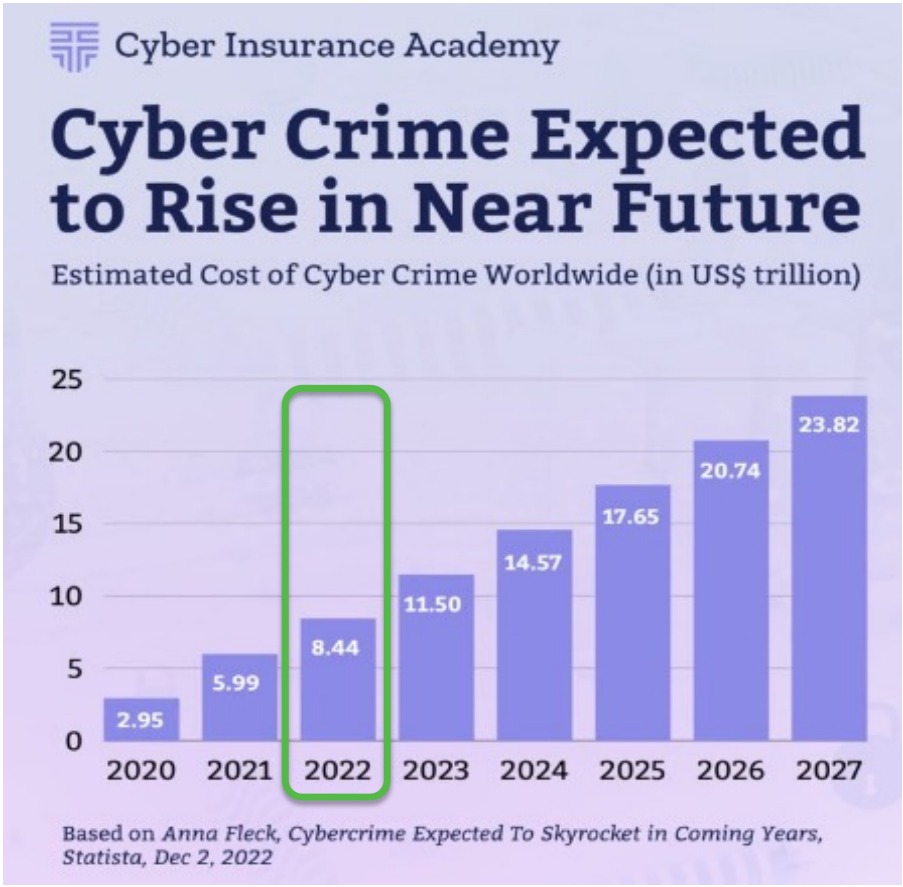
Alternatively, you can..

Nod your head in agreement today.

And then do nothing meaningful.

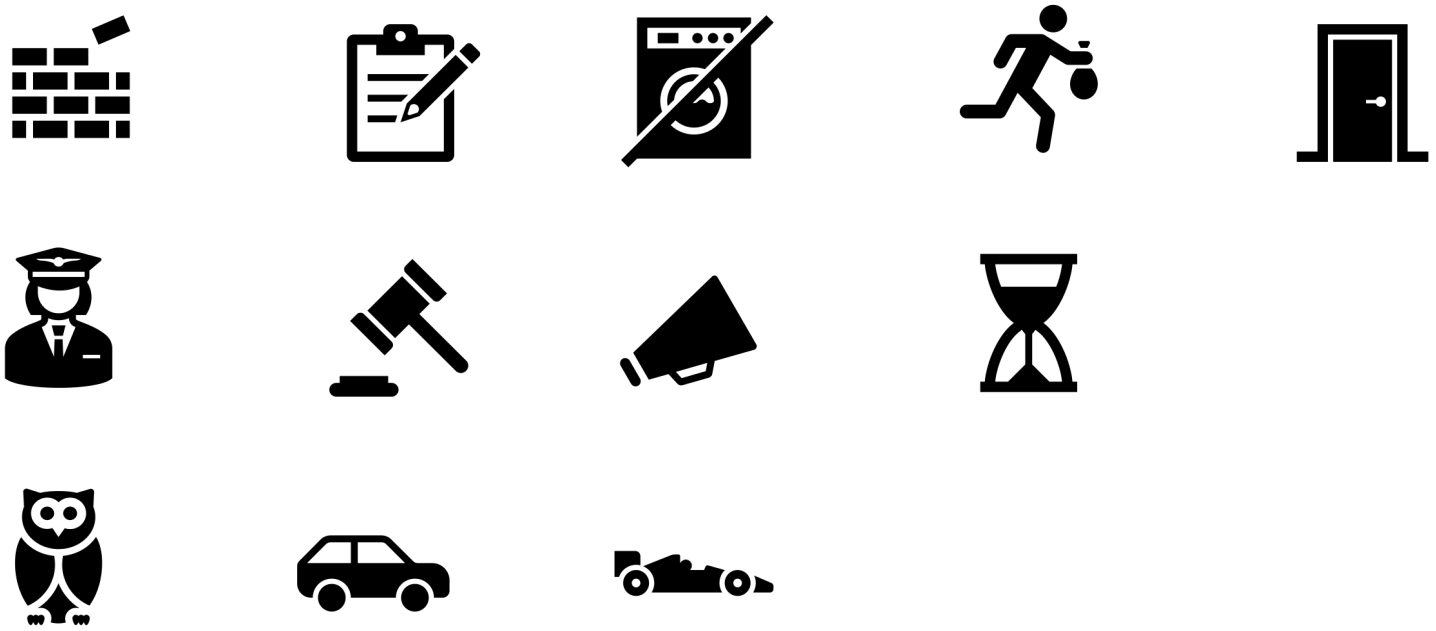
.. And see what happens





The Future: DORA The Enforcer

DORA The Enforcer



DORA Key Points

1. Digital Resilience of FS firms
    1. AND ICT service providers involved in ‘critical’ or ‘important’ processes.

2. Specific Requirements & *Prescribed* Standards for areas such as:
    1. IT risk management
    2. Third Party Risk Management (TPRM) / Outsourcing Risk Management
    3. Incident reporting
    4. Regular Testing – Internal and external audits for many.
    5. Information Sharing

DORA is your new regulatory baseline

Wrap Up

Wrap Up

We have covered:

1. The Past: Central Bank's expectations
   - 2016 Guidance
   - 2020 Dear CEO
   - 2021 Op Resilience and Outsourcing

2. The Present: The common gaps
   - The red flags to watch out for
   - The simple defences
   - How to get started

3. The Future: DORA The Enforcer.

Q&A / Where can you learn more?

Who? Sam Glynn, Code in Motion Ltd

What? **Independent** advisor to help you keep the cyber attackers and regulators from your door.

How? I independently **assess** your current defences using appropriate benchmarks / baselines, and then **guide** you (and your external service providers) on how to close the gaps.

Where?

Website: https://codeinmotion.ie/irishfunds

LinkedIn: https://www.linkedin.com/in/samglynnie/

Cybersecurity for Regulated Firms – Q&A

Paul Burke, Link Group

Sam Glynn, Code In Motion

Disclaimer: The material contained in this document is for marketing, general information and reference purposes only and is not intended to provide legal, tax, accounting, investment, financial or other professional advice on any matter, and is not to be used as such. Further, this document is not intended to be, and should not be taken as, a definitive statement of either industry views or operational practice.

The contents of this document may not be comprehensive or up-to-date, and neither Irish Funds, nor any of its member firms, shall be responsible for updating any information contained within this document.