

Scratch building an incident response capability

Adrian Leung

Head of Information Security

8th March 2017

Secure information **Secure Catalyst**



Agenda

1. Where do we start?
2. Our approach
3. Raising awareness
4. On hindsight
5. Where are we now



1. Catalyst Security & Privacy Programme

Security Foundations	S1. Security Governance	S2. Security Policies	S3. Awareness & Training	S4. Data Protection	S5. Information Classification
Business Process	B1. Compliance	B2. Physical Security	B3. HR Security	B4. Third Party Security	B5. Incident Management
Tools & Technology	T1. Network security	T2. Information Protection	T3. Threat & Vulnerability Assessment	T4. Monitoring & Reporting	T5. Identity & Access Management

1. Where do we start?

Starting fresh

We had no

- Policy, plan or approach
- In-house IR skills
- Clear IR roles, responsibilities, nor team
- Central reporting mechanism
- Monitoring capability
- Visibility of type and volume of incidents (threat landscape)



1. Where do we start?

Hurdles

Other challenges we face

- Budget
- Culture and awareness (e.g. reporting an incident)
- Perception of additional work and value add
- Lack co-ordinated approach



2. Our approach

Key activities to mature our IR capability

Phase 1

- Understand current state
- Centralise reporting
- Develop IR policy and processes
- Raise awareness through phishing campaigns

Phase 2

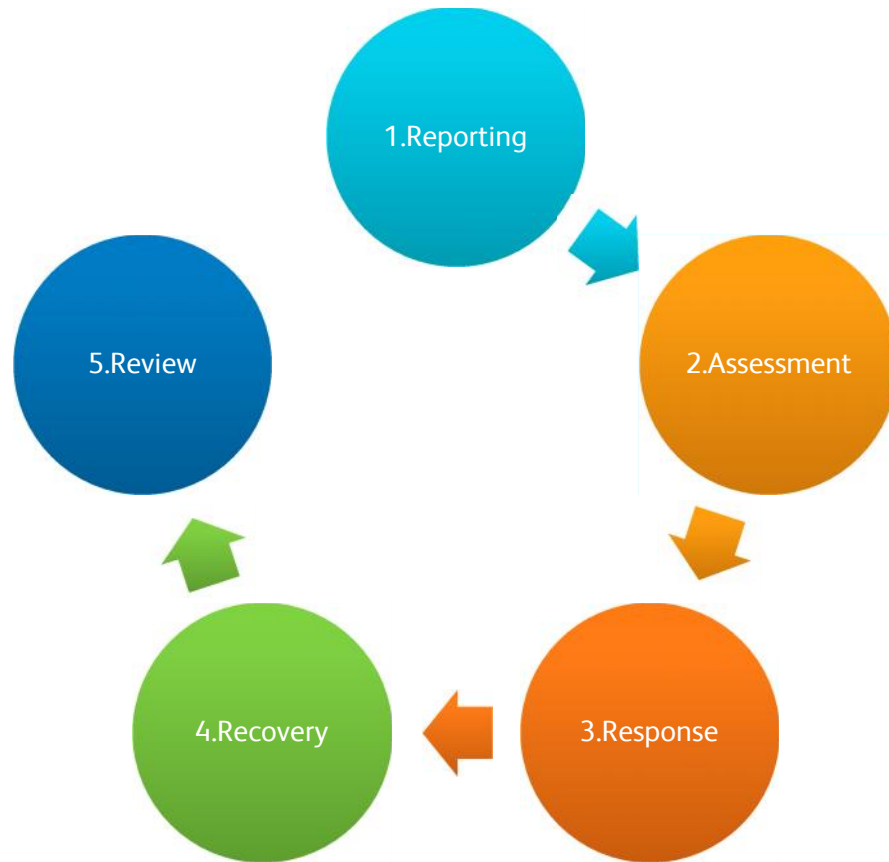
- Develop procedures for common incidents
- Define IR team roles and responsibilities
- Upskill colleagues to triage effectively

Phase 3

- Appoint incident responder for major incidents
- Train in-house IR team
- Continual scenario development
- Test IR plan



3. Incident management process



“A security incident is made up of one or more unwanted or unexpected security events that could very likely compromise the security of information and weaken or impair business operations.”
ISO 27001

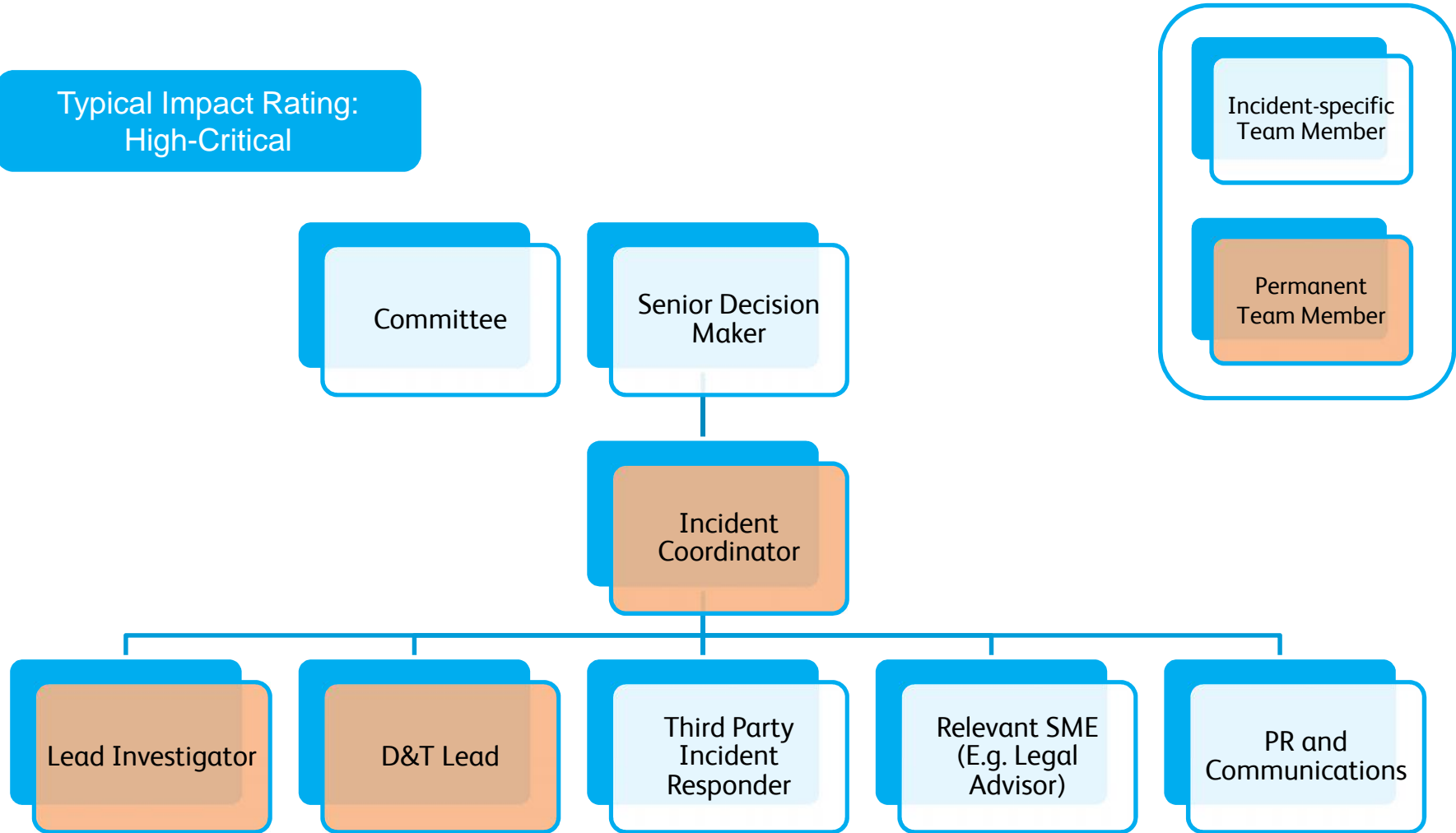
3. Incident management process

Severity ratings

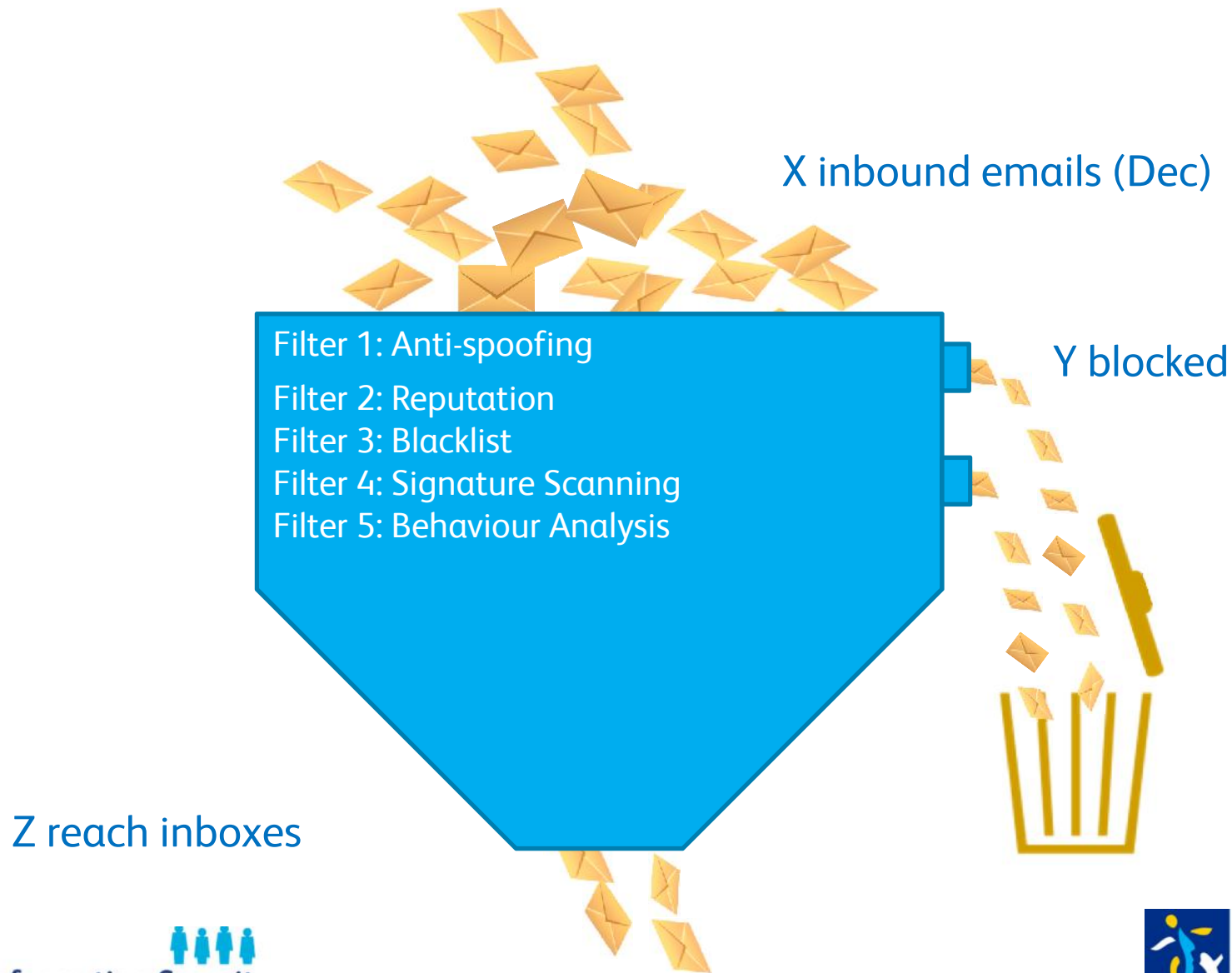
- Critical
- High
- Medium
- Low
- Negligible

3. Incident response team

Typical Impact Rating:
High-Critical



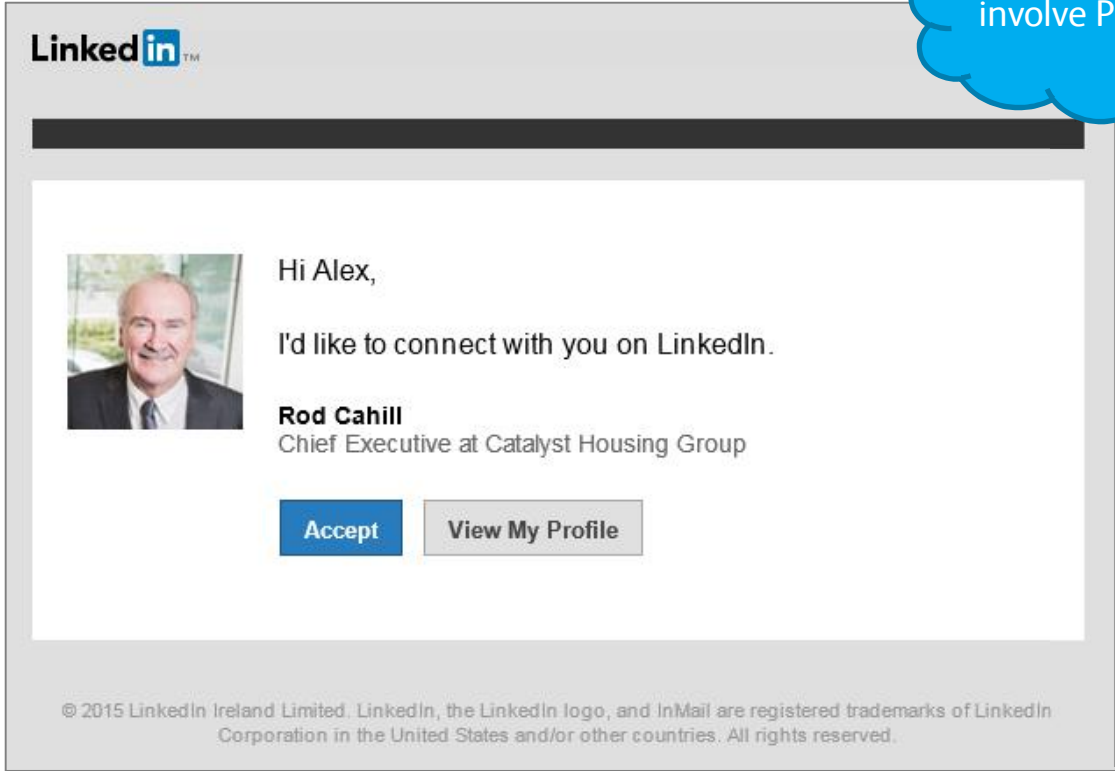
4. Understanding your threats




4. Raising awareness – Gone Phishing

Gone Phishing – “Connect” with the CEO


80 % of incidents involve Phishing




4. Raising awareness – Gone Phishing

 Thu 30/06/2016 12:02
Brite Events <events@briteevents.com>
Your Tickets for the 2016 Housing Innovation Awards

To Adrian Leung

 If there are problems with how this message is displayed, click here to view it in a web browser.

LinkedIn



© 2015 LinkedIn Ireland

Housing Innovation 2016 - Download your tickets now!

Dear Adrian,

The countdown is on for the UK's most anticipated housing event.

You have been allocated tickets because Catalyst housing have been nominated to receive an award. **You must download and print your tickets before the 20th of July.**

With only a few weeks to go, don't miss your opportunity to join colleagues from Catalyst Housing and other housing professionals from across the UK.

A complimentary three course dinner is included in the evening, [view the menu here.](#)

[Find out who else is attending](#) and book a time to network at one of our round table sessions.

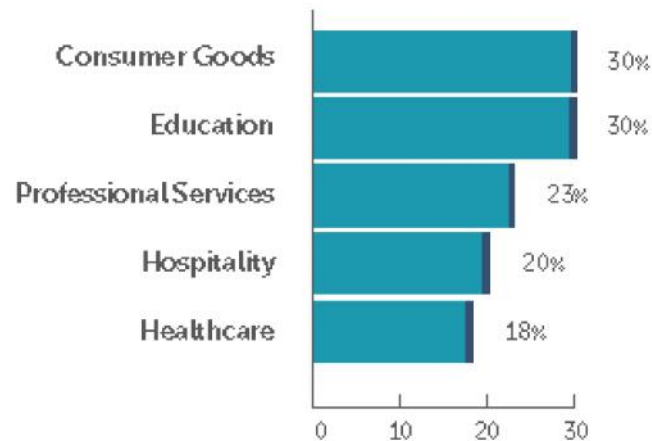
...dule a delivery

4. Raising awareness – Gone Phishing

How Do Different Industries Perform?

For this section, we looked at the three most used template categories (Corporate, Consumer, and Commercial) and used our data to see which industries fell above the average click rates.

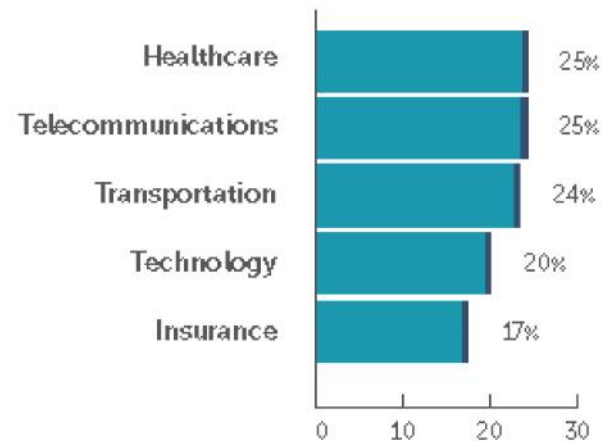
Corporate (15% average click rate)



Corporate Emails

These types of emails look like official corporate communications. Examples include full mailbox notifications, spam quarantines, benefits enrollment messages, invoices, and confidential HR documents.

Commercial (15% average click rate)



Commercial Emails

These are business-related emails that are not organization-specific. Sample topics include shipping confirmations, wire transfer requests, insurance notifications, and auto insurance renewal.

Source: State of the Phish 2017, Wombat Security

4. Raising awareness – ABCs



5. On hindsight

Things easily forgotten along the way



Communicate the incident response process and procedures.



Test the process regularly with scenarios.



Keep stakeholders informed during an incident.

Key IR elements:

- IR Checklist
- Centralised reporting and information logging



5. Where are we now?

Achievements





Housing Security and Privacy Forum 




Forum objectives

A friendly platform to:


- Share and exchange knowledge and good practice
- Discuss common challenges
- Keep abreast of developments in sector
- Collaborate & pool resources -> **Value for Money**
- Develop guidance and standards
- Raise maturity level in sector

LinkedIn Forum


 **Sam Linton**
Data Protection Project Manager at Acis Group ... 5mo

Utility companies


I am still under the impression that we need an agreement with utilities companies to divulge customer details (whether that be on a case by case basis or a more long-standing arrangement). And that it is still at our discretion. Am I wrong? One ene... [Show more](#)

[Like](#) [Comment](#) |  1  4

[View previous comments](#)

 **Jacquie Elliott** Hi Sam, The Information Commissioner's covers disclosing personal data to utilities companies. The condition in 6(1) is met - ie. legitimate interests of the utili

[Like](#) |  1

 **Stephanie Vasey**
Data Manager at Hanover Housing Association ... 1mo

Preparing for General Data Protection Regulations (GDPR) within the Housing Sector

Thank you so much to everyone who attended the GDPR event yesterday. We were really fortunate to have had industry experts who stayed with us all day giving presentations and facilitating the afternoon sessions of round tables. It was great to mee... [Show more](#)

Housing sector forum individual rights slides - 20170131

Slideshare uses cookies to improve functionality and performance, and to provide you with relevant advertising. If you continue browsing the site, you agree to the use of cookies on this



Catalyst Housing



AmicusHorizon

a2dominion

Southern Housing Group



Affinity Sutton

Sanctuary Group

Network Group

housing solutions

Notting Hill Housing

Metropolitan

L&Q
creating places where people want to live



east THAMES

PEABODY

sovereign

Genesis

Knightstone

wm housing group

aster

housingplus
together for the right reasons

The Guinness Partnership

hanover

Circle Housing



CITYWEST HOMES
Classification: Restricted

wdh
Wakefield and District Housing

GreenSquare

Progress
HOUSING GROUP

Thank you!



Want to get in touch?

 Adrian.Leung@chg.org.uk