SFPI Society of Financial Planners Ireland

The Future Risks Of Cyber Liability

BH Consulting

Brian Honan

21st September 2017

Who Am I?

- CEO of BH Consulting – Independent Information Security Firm
- Founder & Head of IRISSCERT – Ireland's first Computer Emergency Response Team
- Special Advisor on Internet Security Europol's CyberCrime Centre (EC3)
- Expert Advisor to European Network & Information Security Agency (ENISA)
- Regularly comments on media stories –
  - BBC, Forbes, Bloomberg, FT, Guardian, Sunday Times

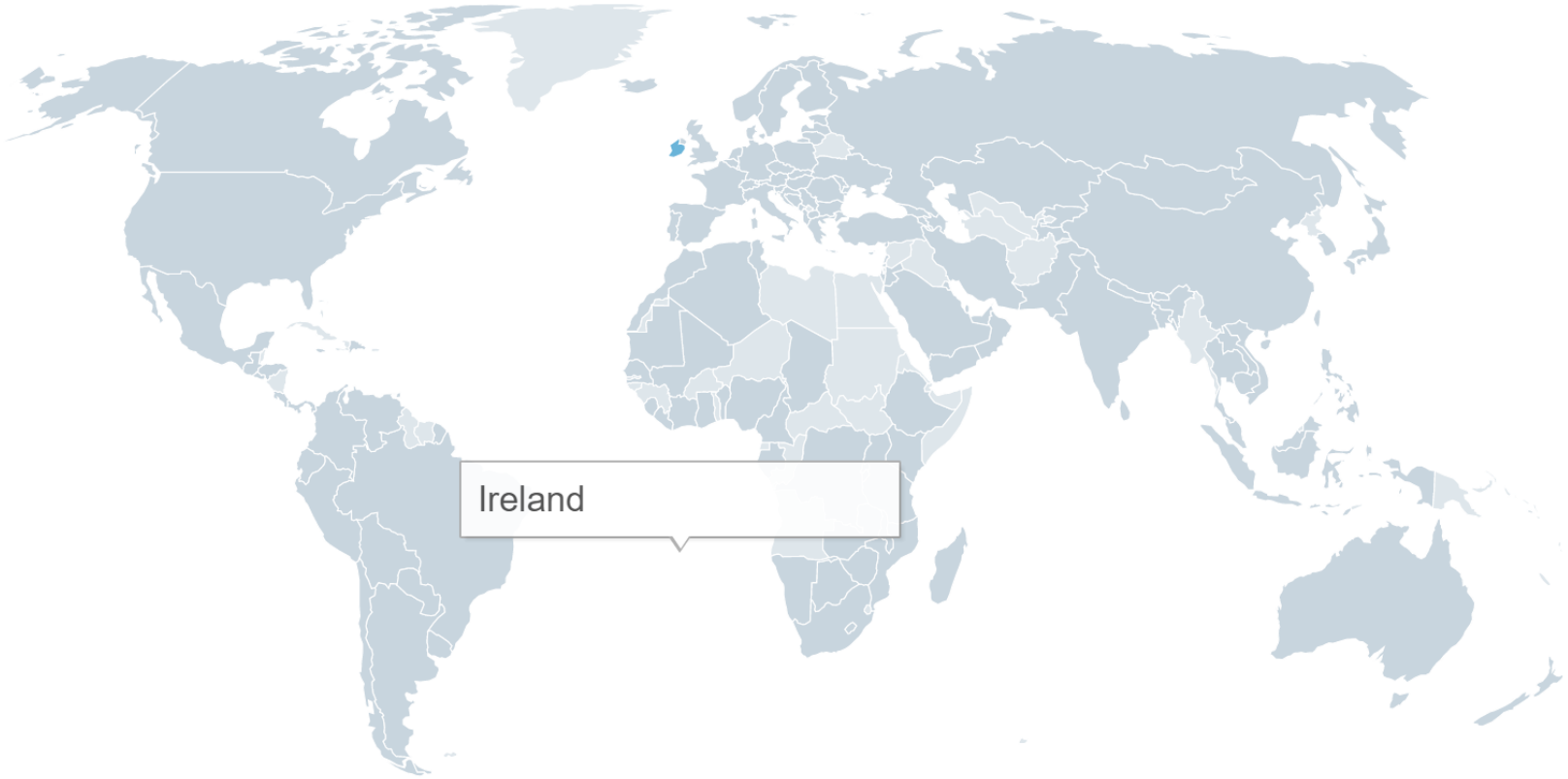
Global Risks of Highest Concern for Doing Business

	Risk	Share
1.	Unemployment or underemployment	36.6
2.	Energy price shock	30.1
3.	Fiscal crises	30.0
4.	Failure of national governance	28.7
5.	Profound social instability	23.8

Ireland ▼

Global Risks of Highest Concern for Doing Business

clear selection



	Risk	Share
1.	Fiscal crises	44.7
2.	Failure of critical infrastructure	42.1
3.	Energy price shock	36.8
3.	Failure of urban planning	36.8
5.	Cyberattacks	34.2
5.	Asset bubble	34.2

The hack, which occurred between May and July, also compromised 182,000 Americans' credit reporting dispute files. | Mike Stewart/AP

Equifax hack exposes 143 million Americans' personal data

By **ERIC GELLER** | 09/07/2017 05:47 PM EDT

Yahoo CEO Marissa Mayer has bonus chopped as a result of massive cyber security hack

Ms Mayer also offered to waive the right to a sizeable annual equity award for this year – an offer that the board accepted

Josie Cox Business Editor | a day ago | 2 comments

Yahoo has endured a turbulent few years and Ms Mayer has repeatedly come under fire for her handling of the 2014 breaches *Getty Images*

Ashley Madison Picture from their website


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 23:37:34
Time Left
02:23:30:20
Your files will be lost on
5/19/2017 23:37:34
Time Left
06:23:30:20
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
Copy
Check Payment
Decrypt

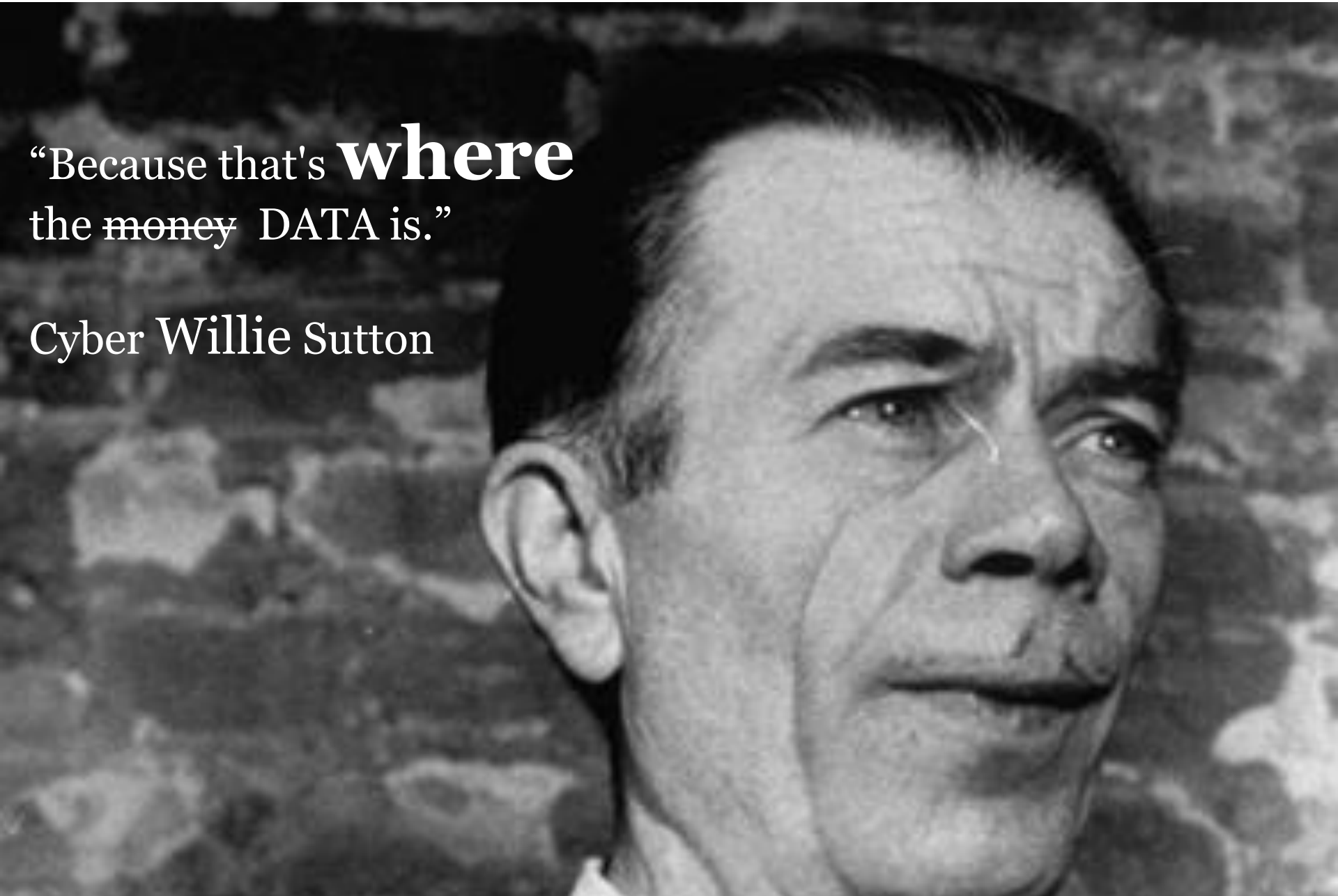
The hack, which occurred between May and July, also compromised 182,000 Americans' credit reporting dispute files. | Mike Stewart/AP

Equifax hack exposes 143 million Americans' personal data

By **ERIC GELLER** | 09/07/2017 05:47 PM EDT

Why Would Someone Want to Hack Me?

Why Would Someone Want to Hack Me?



Cybercrime Marketplace

$1-$6	US Credit card number
$2-$12	UK Credit card number
$5-$50	Medical ID card
$6-$18	Basic identity information
$7	PayPal account with credentials
$50-$500	PayPal verified with balance
$20	DDoS attack from bot army (per hour)
$30	Passwords to consumer credit reports
$50 to $60	Health/medical record
$140	10 million email addresses
$200	Malicious Software Toolkit
$500	20 million SPAMs sent from bot army
$100-$2000	Malware as a Service (MaaS)
$1000-$5000	Online banking accounts with a balance
$10000	0-Day Exploit

Institute of Directors in Ireland

- **93%** of directors rate cyber security as an important issue at board level

- **41%** say there has been a significant increase in the priority placed on cyber security at board level in the past 3 years

- **40%** of organisations have **no** formal cyber security strategy

- **< 25%** of organisations have cyber liability insurance in place

Institute of Directors in Ireland

- **33%** of organisations experienced a cyber breach in the past 2 years with **44%** of organisations selling online have experienced a cyber breach

- **84%** of directors say their organisation will increase spending on cyber security measures over the next 3 years

- **69%** of directors claim their organisation is prepared or very prepared for a cyber breach

Current Issues/Concerns

- DDoS Extortion
- Ransomware
- CEO Fraud

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

Who's behind the breaches?

75% perpetrated by outsiders.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

...alware.

...veraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

Who's behind the breaches?

75% perpetrated by outsiders.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24%

of breaches affected financial organizations.

prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

27% of breaches were discovered by third parties.

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches

15% of breaches

12% Public sect
prevalent b

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

of breaches were discovered by third parties.

Other Cybersecurity Drivers

- EU General Data Protection Regulation
- EU Network & Information Security Directive
- Payment Card Industry – Data Security Standard
- European Central Bank
- European Banking Authority
- Central Bank of Ireland
- Irish National Cybersecurity Strategy

Central Bank of Ireland

*"It is the **board's responsibility to ensure that a firm is properly governed** and **has the necessary processes and systems** to protect the firm and all of its assets"*

And that:

*"an ethos of **effective corporate governance**, coupled with appropriate **I.T. and cyber-security risk management**, can be the foundation of successful protection against cyber-crime. The board should develop a **culture of security and resilience** throughout the firm and ensure that the firm has the necessary **plans in place to deal with both internal and external cybersecurity breaches**".*

"Review of the management of operational risk around cyber-security within the Investment Firm and Fund Services Industry" - September 2015.

Central Bank of Ireland

"We do acknowledge that an effective cybersecurity programme should be reflective of the size, business model, nature and sensitivity of the firm's critical assets. That being said, there are a number of common themes that are pertinent to most or all firms:

- **The Board should have a good understanding of the main risks:**
- **Perform risk assessments and intrusion tests:**
- **Prepare for the successful attacks**:
- **Manage vendor risk:**
- **Gather information and follow best practices:**
- **Educate staff:**
- **Robust IT policies, procedures and technical controls are put in place:**
- **Consider buying cyber-insurance:**

Deputy Governor Central Bank of Ireland, Cyril Roux, to the Society of Actuaries in Ireland Risk Management Conference in September 2015.

What is GDPR?

- The EU General Data Protection Regulation (GDPR) is the update to the EU Data Protection Directive
- Came into Force 24th May 2016
- Will Apply Across All 28 EU Member States

- **25th May 2018**

(Just over 7 months to be ready)

What is GDPR?

- Updates the EU Data Protection Directive with a Strong Focus on Individual's Privacy Rights
- Harmonises the Data Protection Regime Across All 28 EU Member States
- Will Apply Across All 28 EU Member States
- Significant (and Fines) Obligations on Organisations Holding Personal Data

What it Means to The Individual

- The Right to be Informed
- The Right of Access
- The Right to Rectification
- The Right to Erasure
  - Otherwise Known As The Right to Be Forgotten
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object
- Rights in Relation to Automated Decision Making and Profiling

What it Means to Organisations?

- Obtain Clear Consent
- Obtain parental consent if Data Subject Under 16
- Provide a Copy of an Individual's Personal Data on Request
- Erase all Personally Identifiable Records if Requested
- Provide ***"Adequate Security"***
- Privacy Impact Assessments
- One Supervisory Authority to Deal With
- You Can Select your Preferred Supervisory Authority

Mandatory Breach Notifications

- If Personal Data Breach

  “likely to result in a risk to the rights and freedoms of individuals”

- Notify The Supervisory Authority Within **72 Hours** of Becoming Aware of Breach

- If High Risk Breach Likely To Affect Rights and Freedoms of Individuals

  “ *You Must Notify Those Concerned Directly*”

Mandatory Breach Notifications

- The Nature of the Personal Data Breach Including:
  - Categories and Approximate Number of Individuals Impacted;
  - Categories and Approximate Number of Personal Data Records Concerned;
- Contact Details of the Data Protection Officer or Other Contact Point;
- Description of Likely consequences of the Personal Data Breach;
- Description of Measures Taken, or Will be Taken to;
  - Deal with the Breach
  - Measures (if appropriate) Taken to Mitigate any Possible Adverse Effects.

Appoint A Data Protection Officer

- Mandatory For
  - A Public Authority (with some exceptions);
  - Companies with;
    - Large Scale Systematic Monitoring of Individuals,
    - Large Scale Processing of Special Categories of Data
    - Large Scale Processing of Data Relating to Criminal Convictions and Offence
  - Data Protection Officer Must
    - Report to the Highest Management Level of Organisation
    - Operates independently
    - Is not Dismissed or Penalised for Performing their Task.
    - Have Adequate Resources are Provided

Significant Fines

- Supervisory Authority Can Fine;
  - Up to €20,000,000 (or 4% of total annual global turnover, whichever is greater) for the most serious infringements
  - Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover
    - On Top of Fine for the Breach itself

- An Individual(s) Can
  - Complain to Supervisory Authority
  - Right To Compensation
  - Potential for Group Actions

168 Working Days

How To Defend

Security Is An Enabler

Identify Key Data Assets

Establish Policies

Use Existing Frameworks

- Cyber Essentials – Aimed at SMEs
- ISO/IEC 27001:2013 Information Security Standard
  - ISO/IEC/27002:2013 Guidance
- NIST CyberSecurity Framework
- The Center for Internet Security - Critical Security Controls


Security
Awareness
Training

Monitor & Respond

Information Sharing


@BrianHonan
Brian.honan@bhconsulting.ie
www.bhconsulting.ie