Grant Thornton

How to define and respond to fraud risk during COVID-19

What You Need to Know

2 December 2020

Speakers

Paul Jacobs
Partner, Forensic & Investigation Services
T + 353 (0)1 680 5835
E paul.jacobs@ie.gt.com

Sinead O'Neill
Director, Forensic & Investigation Services
T +44 2895 871134
E sinead.oneill@ie.gt.com

Roslyn Lee Symmons
Director, Forensic & Investigation Services
T +353 1 680 5864
E RoslynLee.Symmons@ie.gt.com

Agenda

1. COVID-19 and Fraud Risk
2. External Fraud Risks
3. Internal Fraud Risks
4. Antifraud Toolkit

Poll Question #1

Have you had an internal or external fraud committed on your organisation since COVID-19?

A. Yes

B. No

C. Not sure

Grant Thornton

Fraud - It's not a case of if but when!

Belfast mailbox address used by account holder in Russian money-laundering scheme

Cybercrime in Ireland now double global average with record levels of fraud

Couple jailed for £600,000 VAT fraud

A Slovenian woman has been found guilty of deliberately sawing off her own hand as part of an insurance scam.

HSE feared €7.5m fraud during purchase of 350 ventilators

Former solicitors plead guilty to conspiracy to commit fraud

Man arrested over lucrative international fraud activities in Ireland

800 lockdown benefit fraud claims in Northern Ireland as staff did other work during coronavirus pandemic

Irish man arrested as part of €15m global PPE scam

Ireland: BOI Fined Over €1.6 Million In Relation To Cyber- Fraud Incidents

Coronavirus: Up to £3.5bn furlough claims fraudulent or paid in error - HMRC

The U.K.'s Serious Fraud Office charged three former executives of G4S Care and Justice Services UK Ltd. for conspiring to defraud the Ministry of Justice over several years, the prosecutor said in a statement.

Financial company in Dublin city raided as part of alleged international fraud investigation

Former barrister jailed for three years for theft

Judge says Patrick Russell committed substantial breach of trust

A Belfast accountant who defrauded a care home of more than £1m has been sentenced to 18 months in prison.

How does COVID-19 create/increase fraud risk?

COVID-19 is a field day for fraud, with some factors being:

- Many fraud controls are diminished as organisations limit operations to essential personnel (e.g. IT department, segregation of duties)
- Consumer behaviour has changed (e.g. less cash transactions)
- Millions are stuck at home with COVID-19 worries and arguably more susceptible to scams

The COVID-19 fraud challenge

This pandemic environment is expected to result in an increase in both:

- New COVID-19 related fraud scams
- Existing fraud scams, enabled by COVID-19

Poll Question #2

Has your organisation experienced an increase in fraud due to COVID-19?

A. Yes

B. No

C. Not sure at this time

External vs Internal Fraud

External Fraud covers a broad range of schemes depending on the business being targeted. This type of fraud occurs when an external party such as a vendor, customer or third party commits fraud against the organisation.

Internal Fraud, also called *occupational fraud*, occurs when an employee, manager, or executive commits fraud against his or her employer. Internal Fraud fall into three categories Financial Statement Fraud, Asset Misappropriation and Corruption.

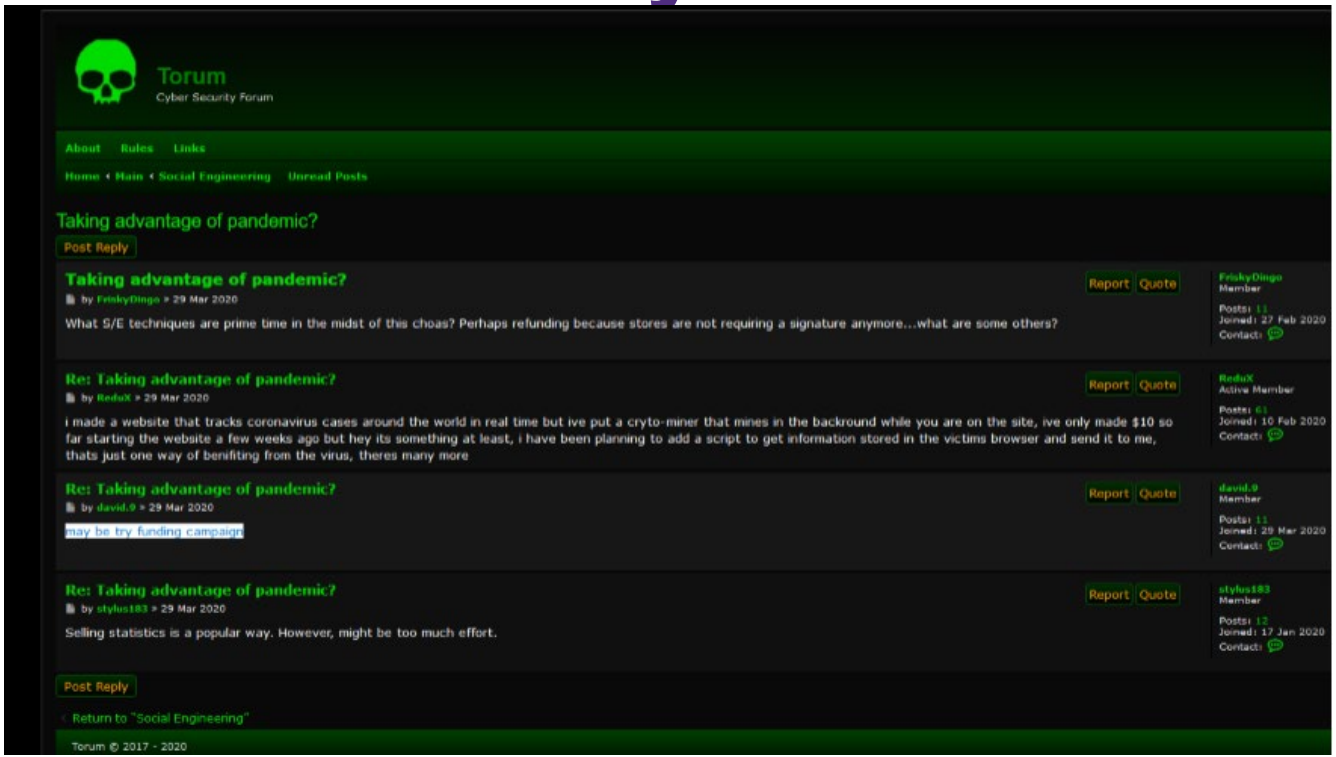
Grant Thornton

External COVID-19 Related Fraud Schemes

How does COVID-19 increase the risk of external fraud?

- People are in a **heightened state of anxiety**, making them more vulnerable to fraud, which fraudsters prey on
- **Chaotic work environments** make it easier to commit fraud as oversight may be more lax
- **Remote work** creates data protection vulnerabilities given than most people's home IT infrastructure is less protected than businesses
- **Dark Web activity** indicates fraud actors are generating new and creative ways to take advantage of the pandemic

Dark Web Activity



Screenshot of dark web forum discussing ways to take advantage of the pandemic

External Fraud Examples

Brandjacking / Imposter Scams	• Using your name, logo and/or brand to reach your customers and/or employees to solicit information or for other disingenuous means. Think a phone call to your customers asking them to update their contact information or a malicious app.
Malware	• Malicious software used to damage devices, steal data, or gain unauthorised access. For example, a fraudster lures an employee to a COVID-19 related website or application which downloads malware onto their work device.
Business Email Compromise	• A fraudster sends a bogus email to the victim masking as a known party with fraudulent payment instructions. With everyone working remotely and in a time of crisis, requests can seem very real and controls may not be closely followed.
Social Engineering	• Similar to BEC, fraudsters prey on this uncertain time and leverage social engineering to persuade victims to transfer funds or divulge sensitive information. The information can be used for identity theft, account takeover or to be monetised in numerous other ways.

What types of Social Engineering should you be on the lookout for?

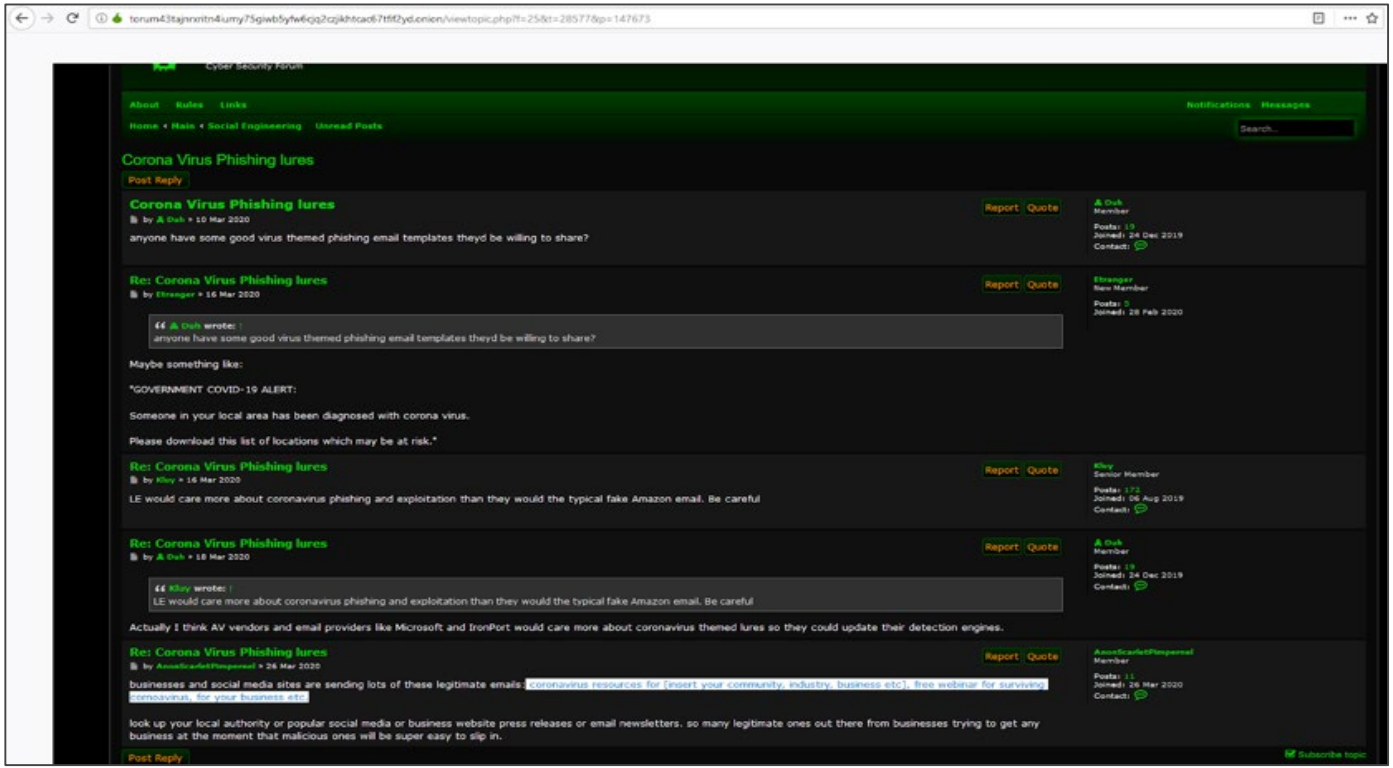
- **Phishing** is any fraudulent communication that purports to be from a legitimate sender to induce a victim to reveal financial data, email credentials, etc.
- **SMiShing** is similar to phishing but uses SMS text messages
- **Spoofing** occurs when a communication from an unknown source (often criminal) is disguised as a known, legitimate source.
- **Deep fake** is an emerging scheme in which a fraudster uses a deep fake audio or video to impersonate a trusted party to trick a victim into sending money to an account owned by the fraudster.

Phishing

- Phishing attacks are at an all-time high due to the crisis
- Common COVID-19 Phishing Schemes:
  - ✓ Verifying personal information to receive funding
  - ✓ Charitable contributions
  - ✓ General financial relief
  - ✓ Airline carrier refunds
  - ✓ Fake cures & vaccines
  - ✓ Fake testing kits

Dark Web: Phishing

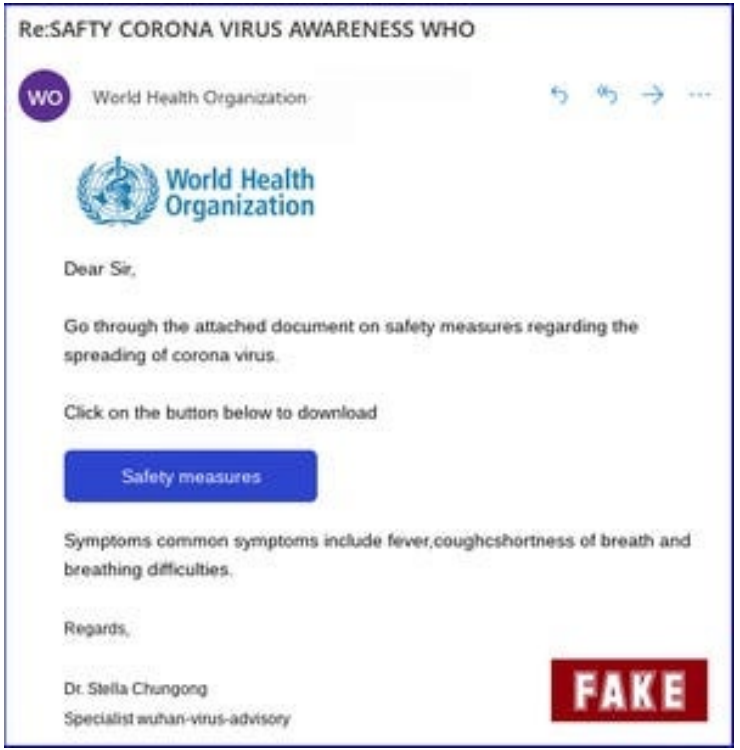
Screenshot of dark web forum with requests for phishing templates re COVID



Example Phishing Email

- One of the firsts scams tied to COVID-19 were phony WHO messages, and they are still circulating.

- It could lead to identity theft if you input the information requested.



External Fraud Examples (cont.)

Synthetic Identity	• A fraudster combines real (typically stolen) and fake information to create a new identity and opens applies for stimulus benefits.
Loan Fraud	• A fraudster applies for a relief loan they are not entitled to. This can be done by forging documents, misrepresenting information or by bribing an official.
Benefit Fraud	• Similar to loan fraud, a fraudster applies for relief benefits they are not entitled to. This can be done by forging documents, misrepresenting information or by bribing an official.
Familiar Fraud / Elder Abuse	• A fraudster uses techniques to woo an elderly individual in order to fraudulently obtain access to their relief benefits. This can be perpetrated by a family member, caretaker or a stranger.

How does government stimulus funding create fraud risk?

Government funding creates ample opportunities for fraud because **the focus will be on getting funds out, with ensuring it gets into the right hands coming second**.

Example fraud schemes include:

- Fraudster poses as a small business owner to secure a loan
- Scammer impersonates an agency offering a loan/benefit through a series of social engineering schemes, with the intent of obtaining beneficiary bank account information
- Fraud actor poses as a consultant, offering stimulus support programs. Falsely collects fees as well as identifying info from individuals and businesses

Other Schemes

- **Charity & Crowdfunding Scams** – a fraudster solicits donations for non-existent or illegitimate charitable organisations
- **Investment Fraud** – a fraudster engages in insider trading, pump & dump schemes, or cryptocurrency scams
- **Seller Scams** – merchants sell products with fraudulent claims or items that are damaged, expired, counterfeit, etc.
- **Buyer Scams** – a fraudster purchases products but cancels payment before the transaction clears but after the product has shipped
- **Healthcare / Provider Scams** – medical providers obtaining patient information for COVID-19 testing and then using that information to fraudulently bill for other tests and procedures.
- **App scams -** scammers are creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information
- **Money Mules** – Fraud actors may exploit unemployed populations as money mules, with fake "work from home" job scams, often posing as processors for COVID-19 charity donations

Poll Question #3

Has your organisation established a plan to deal with COVID-19 related fraud?

A. Yes, we have established a plan and are executing against the plan.

B. We are in the process of establishing a plan.

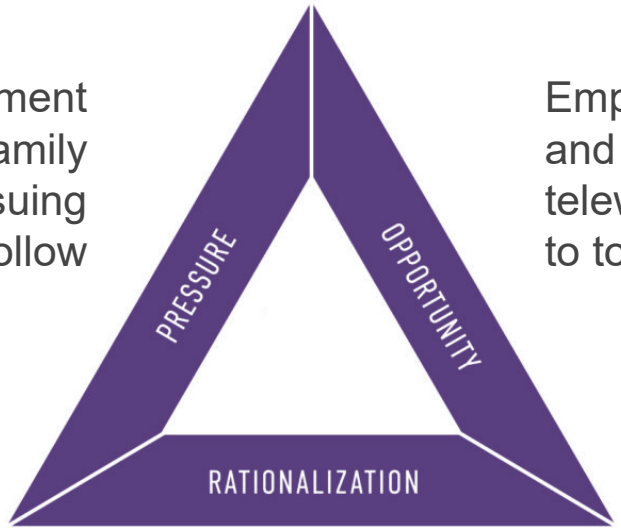
C. We have no established a plan.

Grant Thornton

Internal COVID-19 Related Fraud Schemes

The Fraud Triangle in COVID-19

Employee fears unemployment for themselves and/or family members and the ensuing economic hardship that will follow



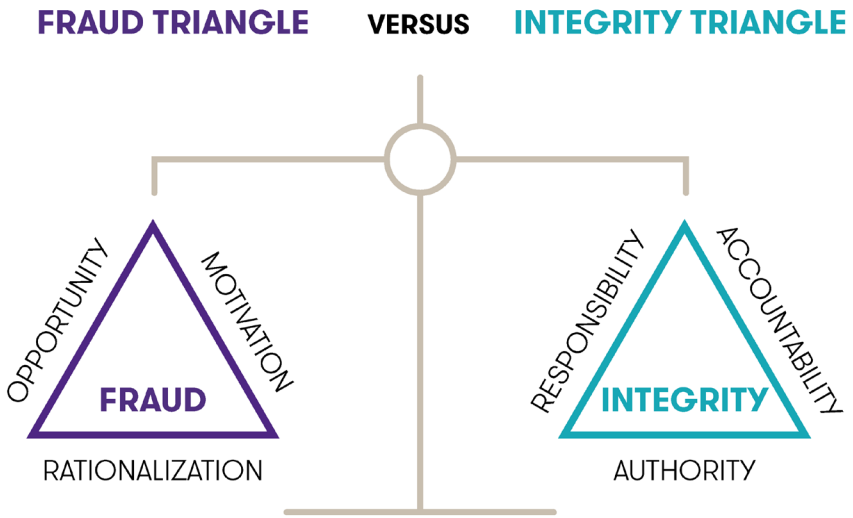
Employee feels unmonitored and empowered in the current telework environment; access to tools like dark web

Employees are able to more easily rationalise fraud when a disaster strikes - *“This is the only way I can support my family”*

The Integrity Triangle

Promoting fraud awareness throughout your organisation from the top down is vital to a creating a **strong anti-fraud culture,** enhancing fraud awareness, and encouraging employees to discuss fraud risks openly and thoughtfully.

There is not a one-size-fits-all model when it comes to promoting fraud awareness. It is important for every organisation to tailor these efforts to be relevant to its **specific fraud risks** and the strategic goals of the FRM program.



Serving as the counterbalance to the **Fraud Triangle**, the **Integrity Triangle** emphasises the values that encourage people to do what is right for the organisation.

Internal Fraud Examples

Benefit Schemes	• An employee misrepresents information to achieve a higher payout or increase benefits. For example, many organisations are offering additional benefits during this time for childcare or other costs, which an employee might exploit for personal gain.
Insider Threat	• An employee with access to sensitive information, such as customer records, sells the account information on the dark web.
Asset Misappropriation & Theft	• An employee uses a company asset for personal purposes or reports an item stolen, when in reality they sell it for a profit.
Corruption	• An employee may bribe an official or collude with another party to defraud the organisation to make up for lost personal income or to obtain stimulus funding.

Poll Question #4

What is your greatest COVID-19 fraud concern?

A. External Threat
B. Insider Threat
C. Other

Poll Question #5

What do you see as the key frauds in the current environment?

A. Phishing
B. Business Email Compromise
C. Asset misappropriation
D. Financial Statement Fraud
E. Bribery
F. Other

Grant Thornton

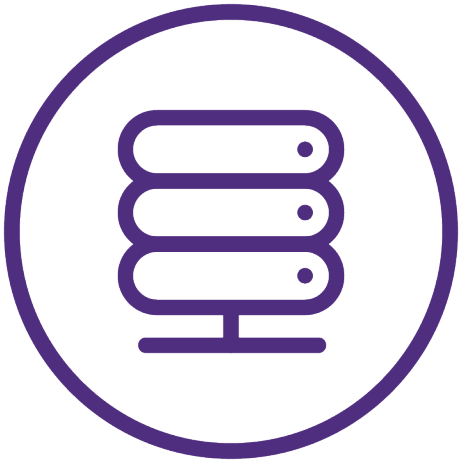
Antifraud Toolkit: Steps to Combat COVID-19 Related Fraud Schemes

Step 1: Champion

Designate an anti-fraud champion in your organisation.

This person should have accountability for all pandemic-related anti-fraud programs.

Step 2: Systems

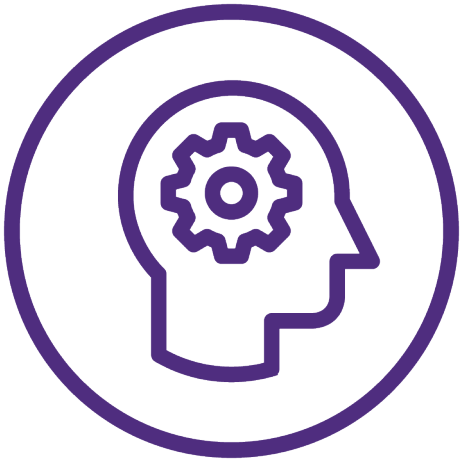


Update core systems.

Current systems may not be well suited to capturing adequate data for new procedures. Plan to adapt current systems or improvise new ones to suit the new process.

Step 3: Think like a fraudster

In these uncertain times, it is even more important to be proactive in identifying new threats.



Step 4: Analytics

Leverage analytics.

In particular, unsupervised detection techniques work best in uncertain times. Anomaly detection, network analytics, and expert rule systems can all add immediate value.

Step 5: Iterate

Iterate and adapt.

Fraud detection is not a “set-and-forget” process. Expect the threat landscape to evolve over time.

COVID-19 Antifraud Toolkit Summary

Step 1. Designate an anti-fraud champion in your organisation. This person should have accountability for all pandemic-related anti-fraud programs.

Step 2. Update core systems. Current systems may not be well suited to capturing adequate data for new procedures. Plan to adapt current systems or improvise new ones to suit the new process.

Step 3. Ideate fraud schemes. In these uncertain times, it is even more important to be proactive in identifying new threats.

Step 4. Leverage analytics. In particular, unsupervised detection techniques work best in uncertain times. Anomaly detection, network analytics, and expert rule systems can all add immediate value.

Step 5. Iterate and adapt. Fraud detection is not a “set-and-forget” process. Expect the threat landscape to evolve over time.

Poll Question #6

Which step of the COVID-19 toolkit will your organisation find most challenging to implement?

A. Step 1: Champion
B. Step 2: Systems
C. Step 3: Ideation
D. Step 4: Analytics
E. Step 5: Iterate

Next step – Anti Fraud Playbook

Fraud Risk Governance: The organisation establishes and communicates a Fraud Risk Management program

Fraud Risk Assessment: The organisation performs comprehensive fraud risk assessment

Fraud Control Activity: The organisation selects, develops, and deploys preventive and detective fraud control activities

Fraud Investigation & Corrective Action: The organisation establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective

Fraud Risk Management Monitoring Activities: The organisation selects, develops, and performs ongoing evaluations

Any final questions?

Please contact one of our Core Forensic team, who between them have over 110 years of experience in Forensics:

Paul Jacobs
Partner, Forensic & Investigation Services
T + 353 (0)1 680 5835
E paul.jacobs@ie.gt.com

Roslyn Lee Symmons
Director, Forensic & Investigation Services
T +353 1 680 5864
E RoslynLee.Symmons@ie.gt.com

Sinead O'Neill
Director, Forensic & Investigation Services
T +44 2895 871134
E sinead.oneill@ie.gt.com

Patrick D'arcy
Director, Forensic & Investigation Services
T + 353 (0)1 680 5709
E Patrick.darcy@ie.gt.com

Andrew Harbison
Director, Forensic & Investigation Services
T +353 (0)1 680 5766
E Andrew.harbison@ie.gt.com

Mike Harris
Partner, Cyber Security Services
T +353 (0)1 6805 835
E Mike.harris@ie.gt.com

Grant Thornton

Thank you for attending

Grant Thornton