Cyber Security

Feeding the Ransom Beast

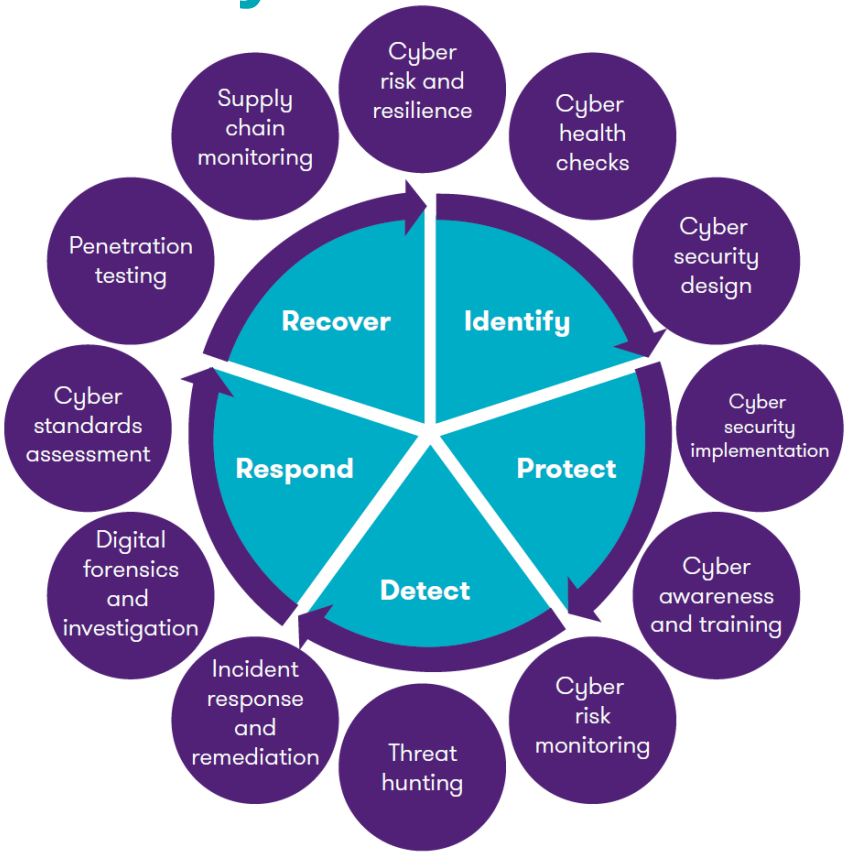
Vijay Rathour
Partner, Grant Thornton
Digital Forensics Group

Grant Thornton

About Grant Thornton

The Best Defence is a Good Offence

Structuring Security



Dear Sir / Madam,

I write to inform you that the GOVERNMENT OF UNITED STATES in conjunction with International Monetary Fund (IMF), has resolved to refund each victim of scam (Advance Fee FRAUD) the sum of $7,500.000 (Seven Million Five Hundred Thousand Dollars only)

On that note, I seek your consent to collaborate with me so that I will put your name as one of the victims entitle and legible for this refunds for our mutual benefits. If you are interested in actualizing this deal with me respond back urgently with your below details to enable me put your name among those that will benefit from the refund this month.

1 Your full names/ address. 2 Your phone number. 3 Your age/sex and occupation.

Please note that the process of filing for this refund is risk free and has nothing to do with illegality because I have perfected every plan for the smooth processing of the refunds.

Bear in mind that our working ratio shall be 50% each as soon as we get the refund in your name.

Email : mskristalinageorgieva2@gmail.com

Yours Faithfully, Ms. Kristalina Georgieva Managing Director International Monetary Fund

Dear Sir / Madam,

I write to inform you that the GOVERNMENT OF UNITED STATES in conjunction with International Monetary Fund (IMF), has resolved to refund each victim of scam (Advance Fee FRAUD) the sum of $7,500.000 (Seven Million Five Hundred Thousand Dollars only)

On that note, I seek your consent to collaborate with me so that I will put your name as one of the victims entitle and legible for this refunds for our mutual benefits. If you are interested in actualizing this deal with me respond back urgently with your below details to enable me put your name among those that will benefit from the refund this month.

1 Your full names/ address. 2 Your phone number. 3 Your age/sex and occupation.

Please note that the process of filing for this refund is risk free and has nothing to do with illegality because I have perfected every plan for the smooth processing of the refunds.

Bear in mind that our working ratio shall be 50% each as soon as we get the refund in your name.

Email : mskristalinageorgieva2@gmail.com

Yours Faithfully, Ms. Kristalina Georgieva Managing Director International Monetary Fund

1

↑ 44%

2021: 3 (40%)

Cyber incidents

(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)

3

↑ 25%

2021: 6 (17%)

Natural catastrophes

(e.g. storm, flood, earthquake, wildfire, weather events)

2

↓ 42%

2021: 1 (41%)

Business interruption

(incl. supply chain disruption)

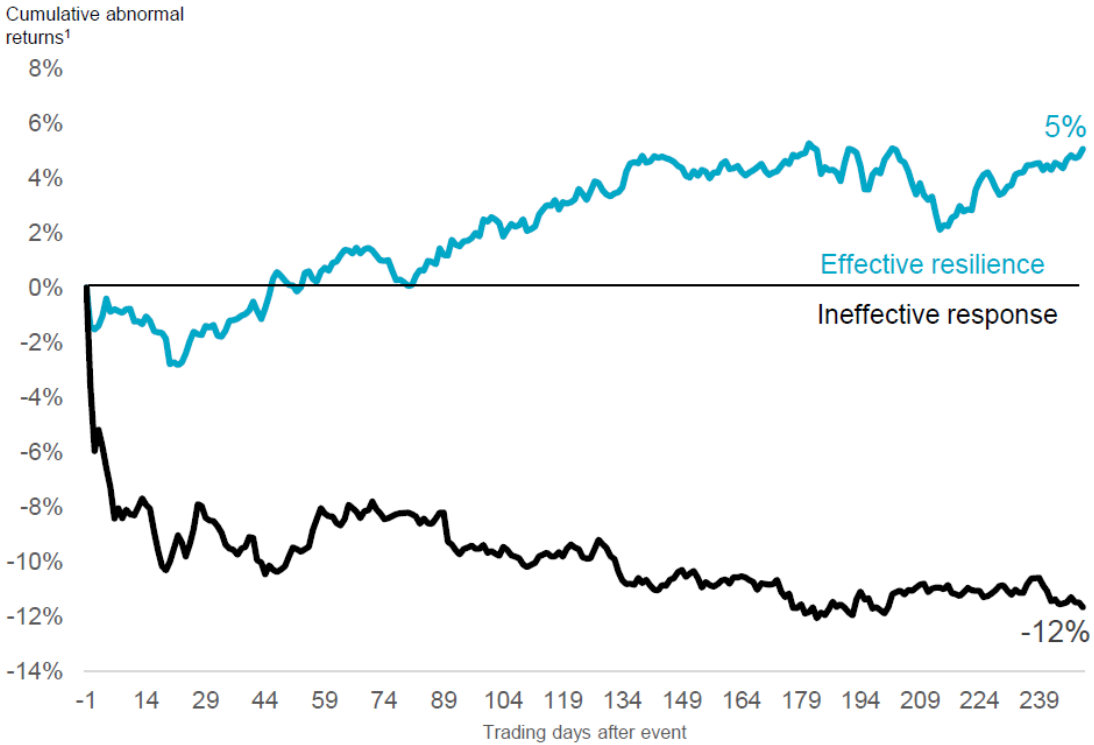
Allianz Risk Barometer 2022

Preparing for Crisis

In Summary:

The Evolving Cyber Threat Landscape

The Cost of Recovery:
Factors leading to a successful crisis



Key success factors:

1 The strength of a leadership's response.

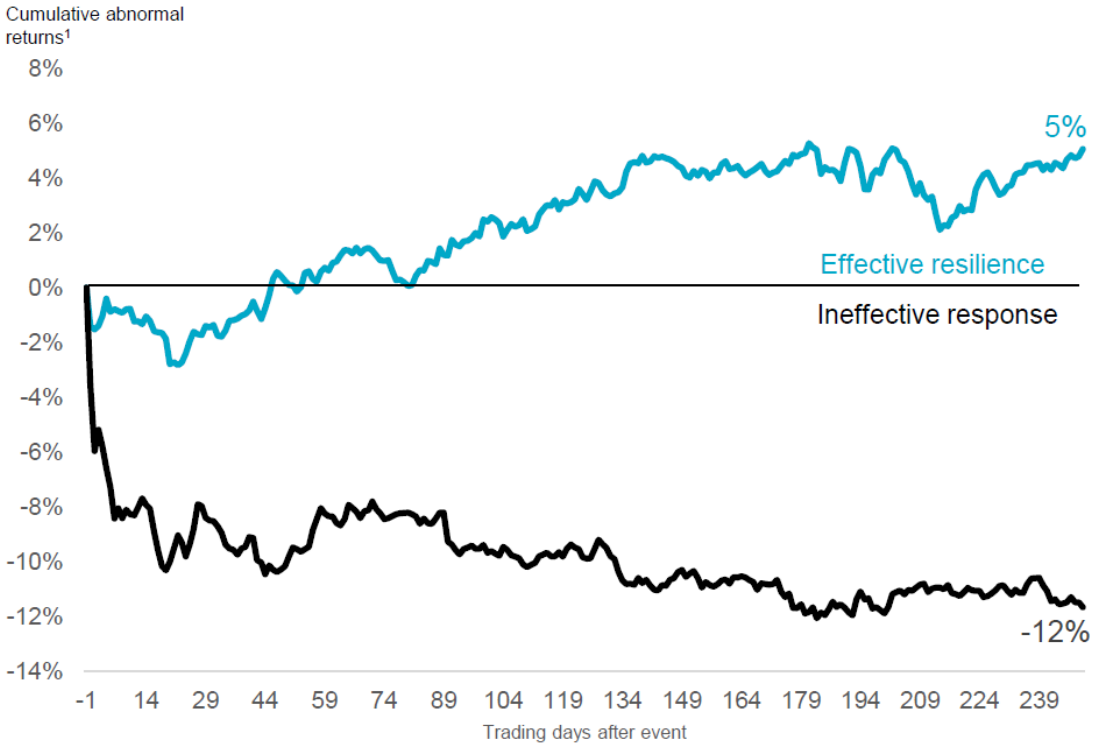
2 Swift, accurate, and transparent communication.

3 Attempts to conceal facts can have a major negative impact.

4 A flexible and agile supply chain.

5 Tested crisis arrangements.

The Cost of Recovery:
Factors leading to a successful crisis



Key success factors:

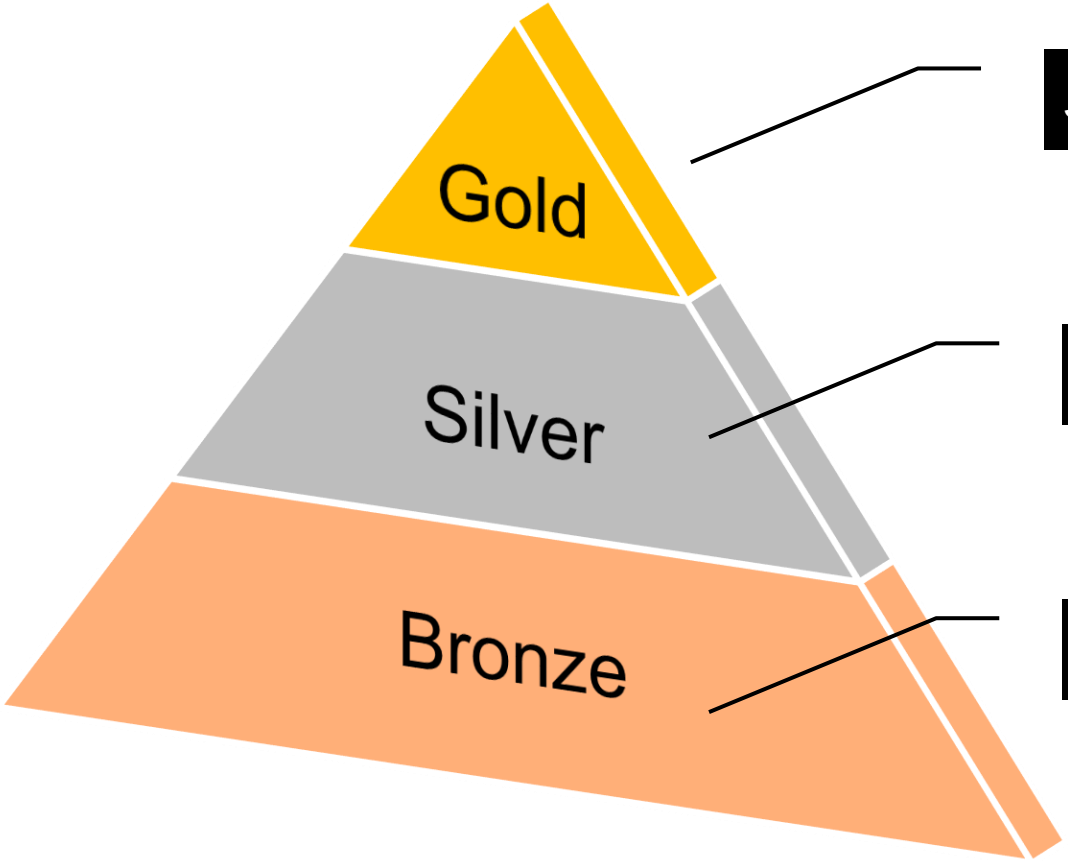
1. The strength of a leadership's response.
2. Swift, accurate, and transparent communication.
3. Attempts to conceal facts can have a major negative impact.
4. A flexible and agile supply chain.
5. Tested crisis arrangements.

The Hardest Question to Answer?

Comms Damage Control

- *“How long did you know about it before you decided to do something?”*
- *“If you had acted sooner, could this crisis have been avoided?”*
- *“If you didn’t know that something was wrong, why not?”*
- *“Isn’t it your job to know about potential crises?”*
- *“If you did know about it, why didn’t you act earlier?”*
- *The Charity Commission*

Emergency Response Team Structure



Strategic: What we intend to do

Tactical: How we intend to do it

Operational: doing it

Remember


Everyone has a plan
until they get punched
in the face

Vijay Rathour

Partner – Digital Forensics

Vijay.Rathour@uk.gt.com

Tel: +44 (0)7788 418 652

Digital Forensics & Investigations
Electronic Disclosure Consultancy
Cyber Defence & Response
Data Breach Support Hub (24 Hours)
+44 20 7865 2552
cir@uk.gt.com

Grant Thornton

Staying Safe Hints and Tips

Staying Secure

- **Phishing Attacks & Scams**
  - train staff to be alert
    - spelling errors, change of bank account etc
  - control websites they can access
  - use virus killers and malware scanners
  - change passwords if anything suspicious occurs
  - consider two factor authentication

Staying Secure

- **Your Mobile Workforce**
  - encrypt mobiles / laptops where possible
  - enable password / fingerprint controls
  - use mobile device management to wipe devices
  - keep devices patched
  - keep an inventory and alert for lost devices
  - change passwords regularly, but not too often

Staying Secure

- **Monitor and Limit Malware Damage**
  - use virus killers and malware scanners
  - use effective firewalls (change passwords!)
  - control apps that can be installed
  - patch regularly (software & firmware)
  - use endpoint protection / block USB sticks
  - use Mobile Device Management tools
  - use VPNs where possible

Staying Secure

- **Backup your data and BCP**
  - identify your sensitive and valuable data
  - backup (in a separate location) necessary data
  - consider use of cloud infrastructure
  - ensure all data is encrypted (cloud and local)
  - check your networks: not too connected
  - test your protocols – **assume the worst**

The hardest question to answer…

How long did you know, and what did you do about it?

1) The speed of response is critical in ensuring you recover quickly and protect your reputation.

2) The moment you respond is the moment your rebuild begins

3) No-one knows everything on day one

4) Ensure you have functioning crisis response team and clear chain of command

5) You are not alone: know your insurance policies, and who to bring in externally to assist (IT resource, legal support, communications support).