HISCOX

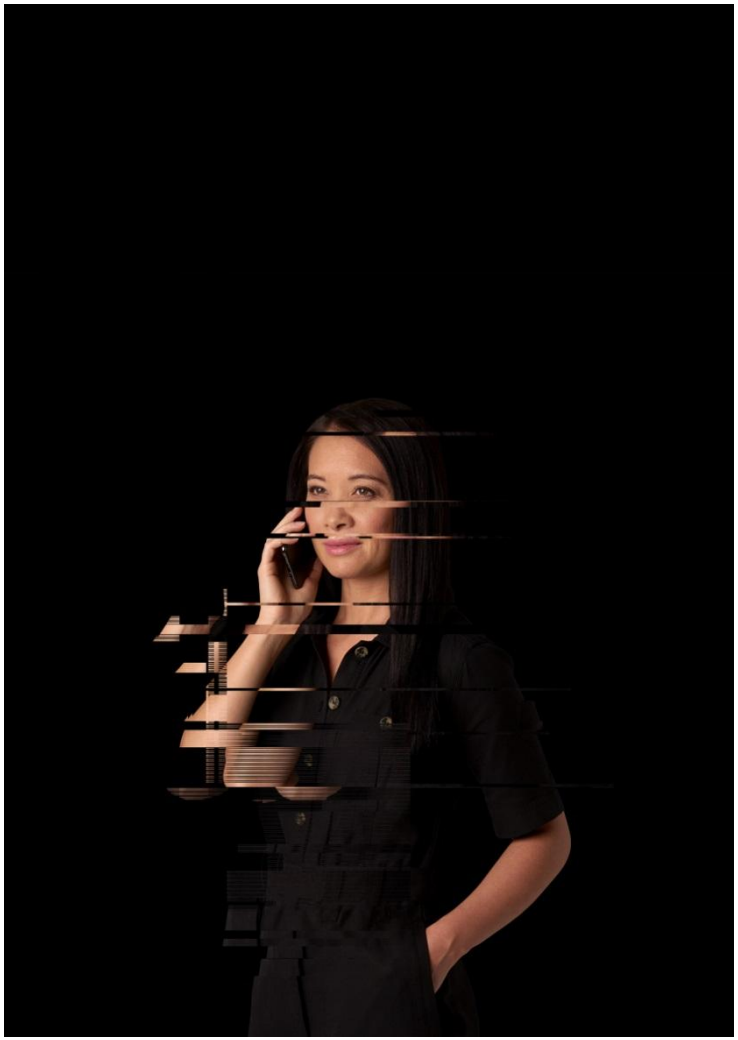
# Fraud in cyber space

## How are criminals digitising, and what are the risks of insurance fraud against cyber policies?

Stephen Ridley, Cyber Underwriting Manager

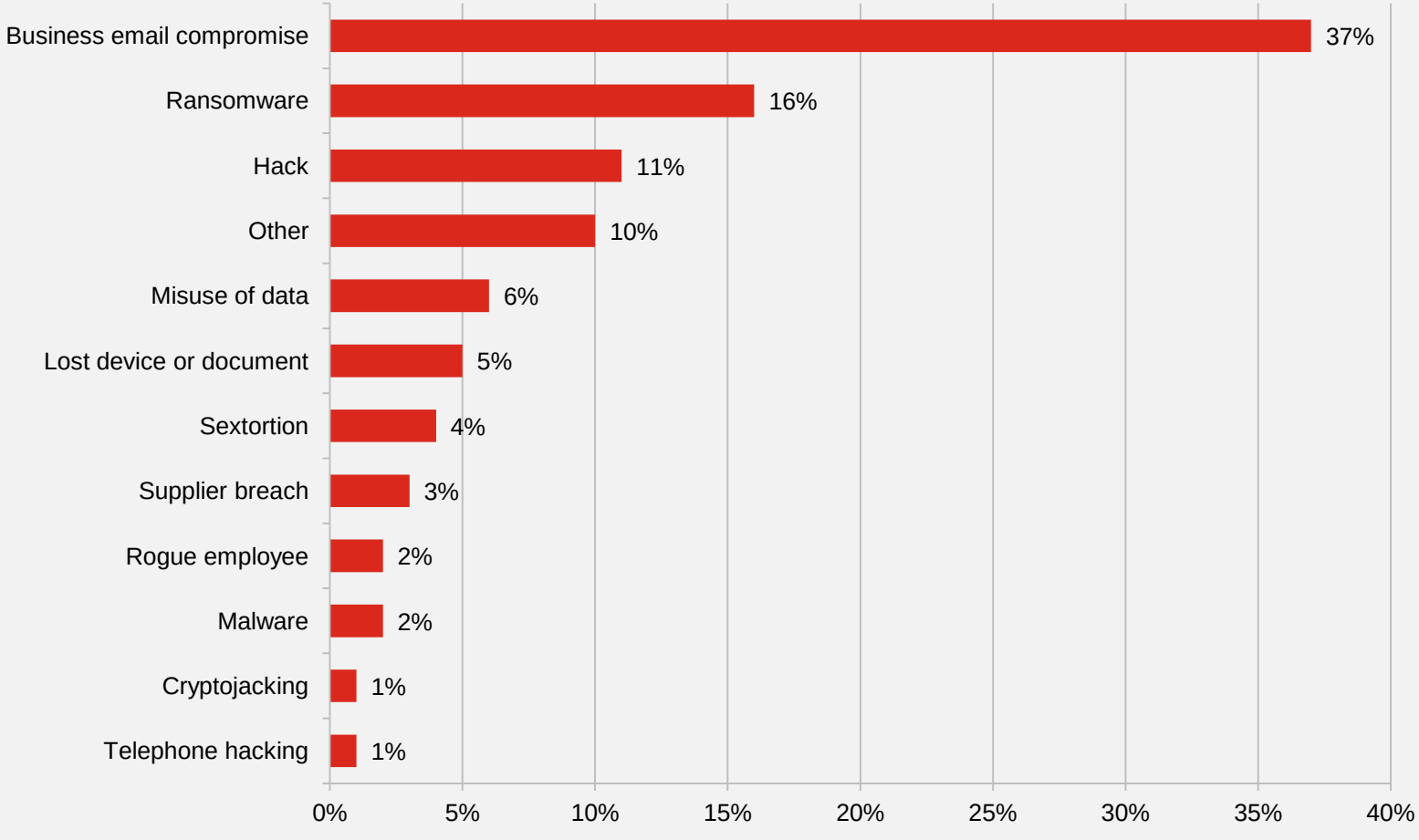
# Fraud in cyber space
## Agenda

- Cyber claim trends
- Case studies
- Consideration of fraud against cyber policies



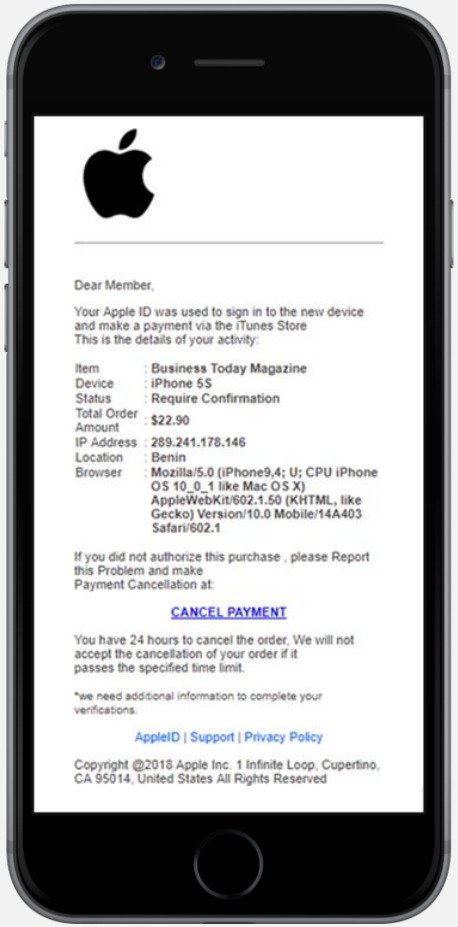
# Cyber claims in 2018
## What did we see?

HISCOX
CYBERCLEAR®



# Cyber claims in 2018
## Business email compromise

HISCOX
CYBERCLEAR®



Dear Member,

Your Apple ID was used to sign in to the new device and make a payment via the iTunes Store
This is the details of your activity:

| | |
|---|---|
| Item | : Business Today Magazine |
| Device | : iPhone 5S |
| Status | : Require Confirmation |
| Total Order Amount | : $22.90 |
| IP Address | : 289.241.178.146 |
| Location | : Benin |
| Browser | : Mozilla/5.0 (iPhone9,4; U; CPU iPhone OS 10_0_1 like Mac OS X) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Mobile/14A403 Safari/602.1 |

If you did not authorize this purchase , please Report this Problem and make
Payment Cancellation at:

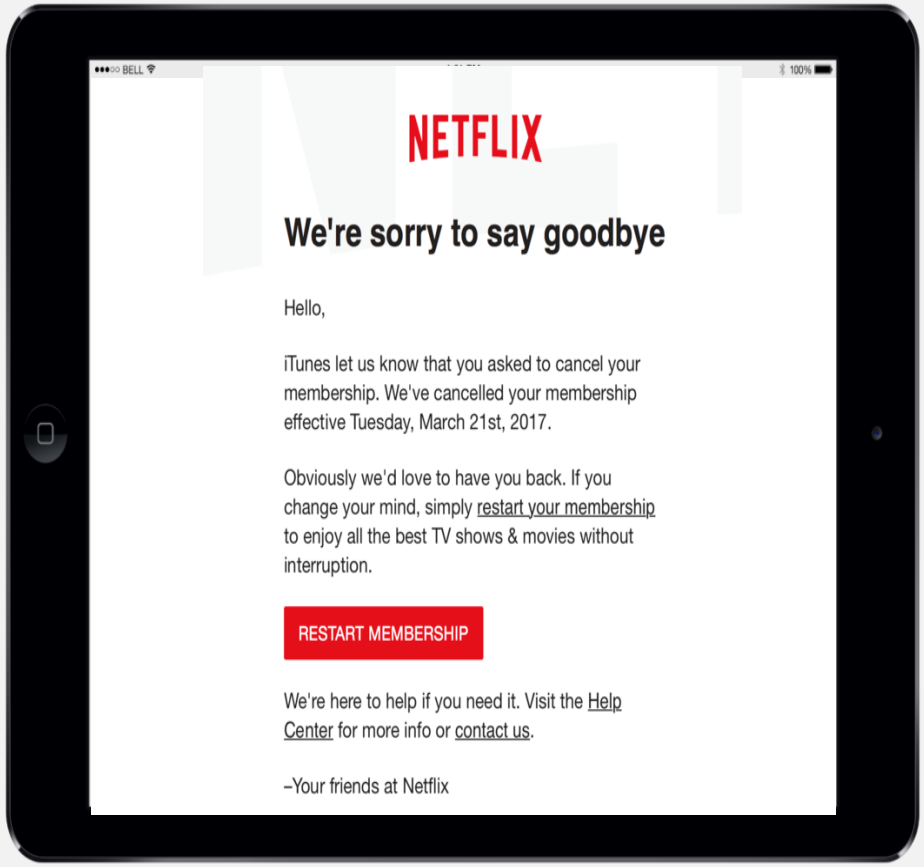
CANCEL PAYMENT

You have 24 hours to cancel the order. We will not accept the cancellation of your order if it passes the specified time limit.

*we need additional information to complete your verifications.

AppleID | Support | Privacy Policy

Copyright @2018 Apple Inc. 1 Infinite Loop, Cupertino, CA 95014, United States All Rights Reserved



NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

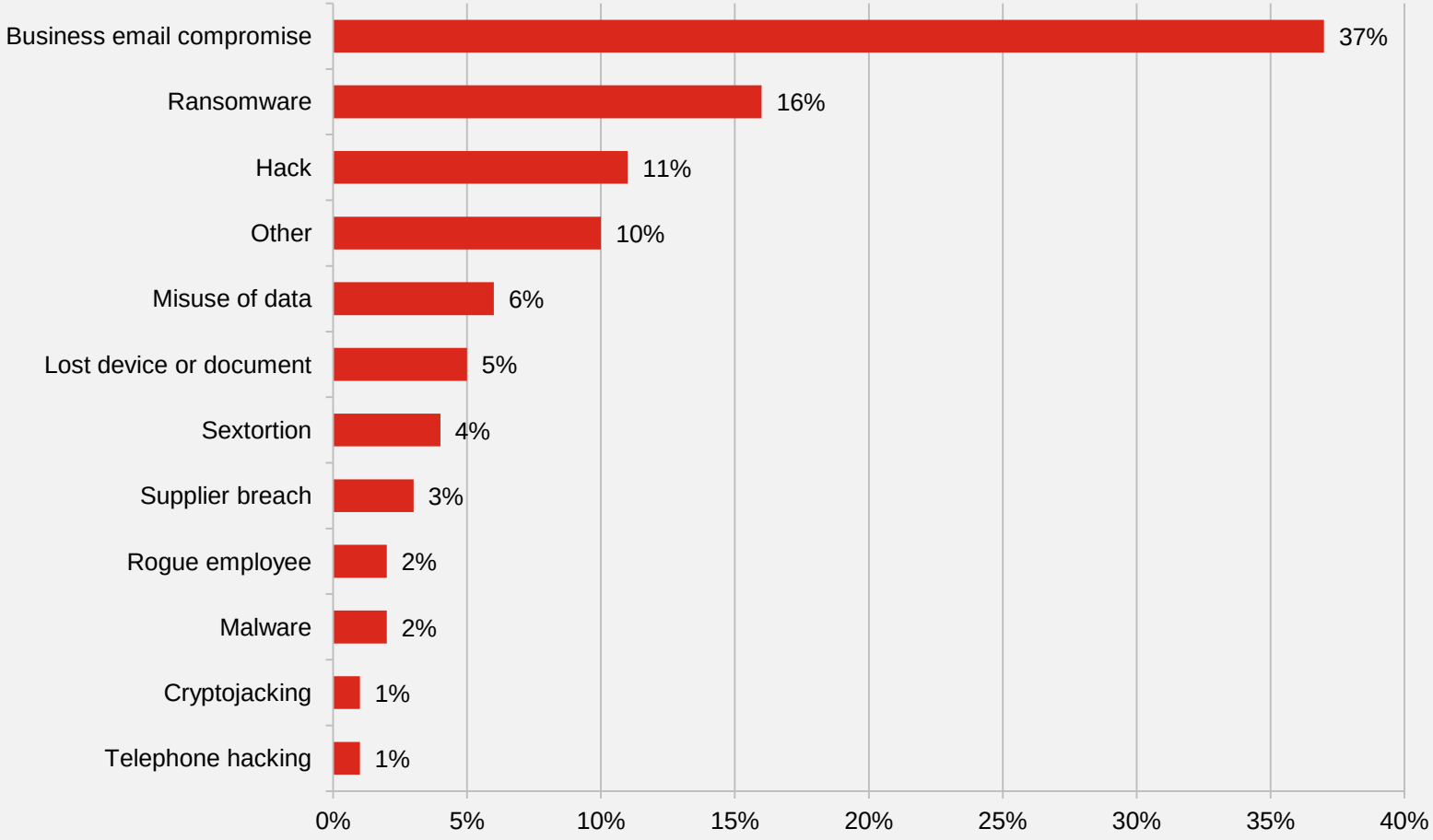
RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

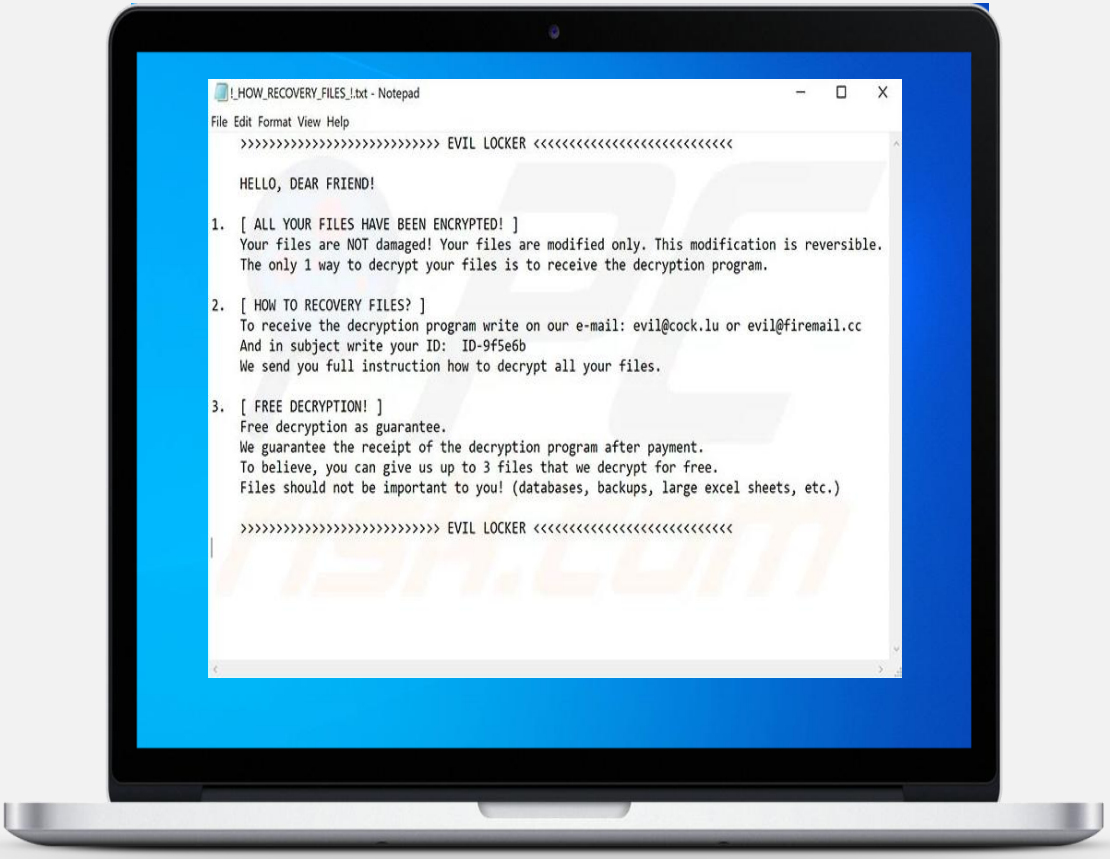
# Cyber claims in 2018

HISCOX
CYBERCLEAR®



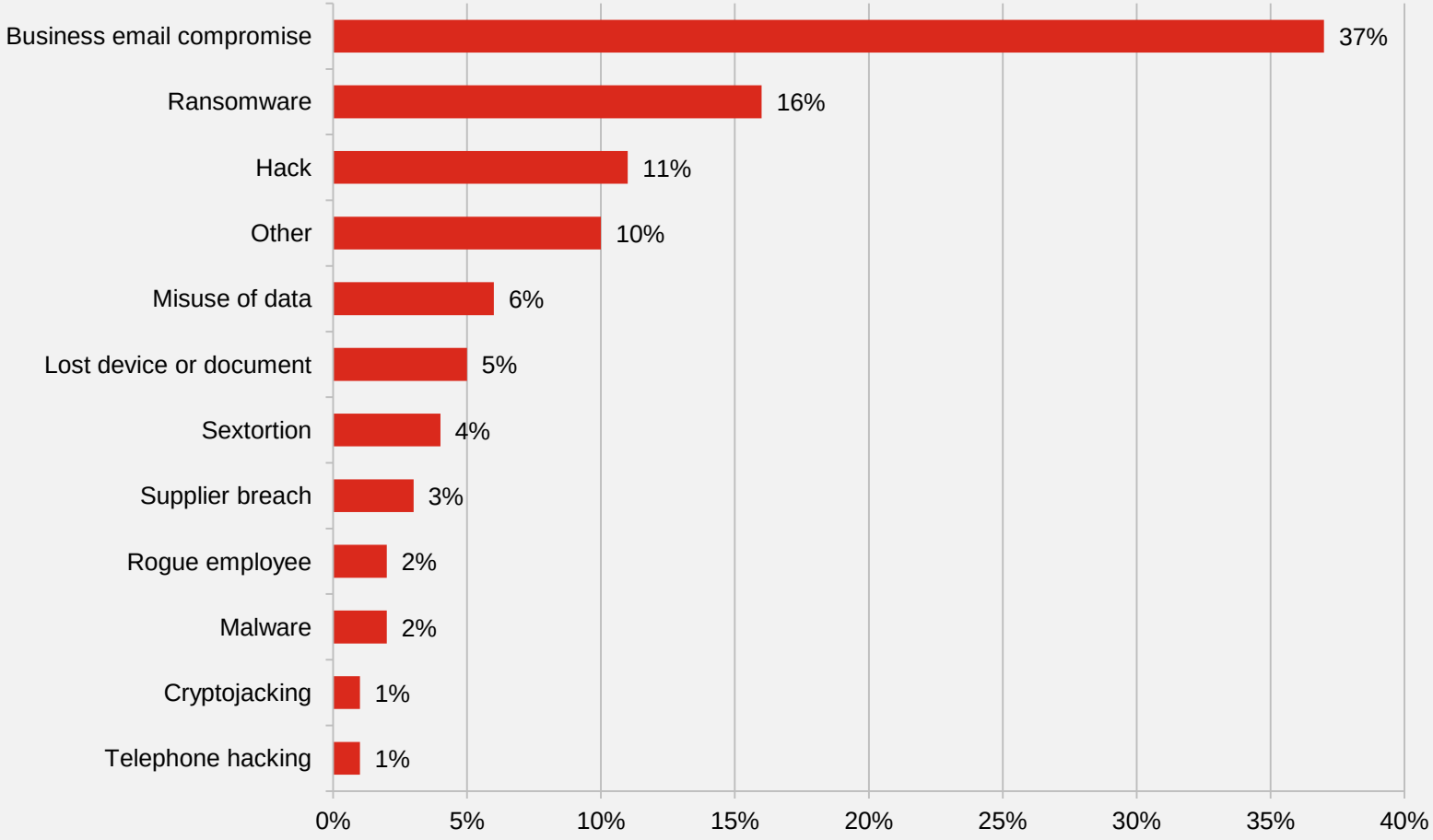
# Cyber claims in 2018
## Ransomware

HISCOX
CYBERCLEAR®



# Cyber claims in 2018

HISCOX
CYBERCLEAR®



# Cyber claims in 2018
## Sextortion

HISCOX
CYBERCLEAR®

Hello!

I'm a programmer who cracked your email and device a few months ago. You entered a pass on one of the sites you visited, and I intercepted it.

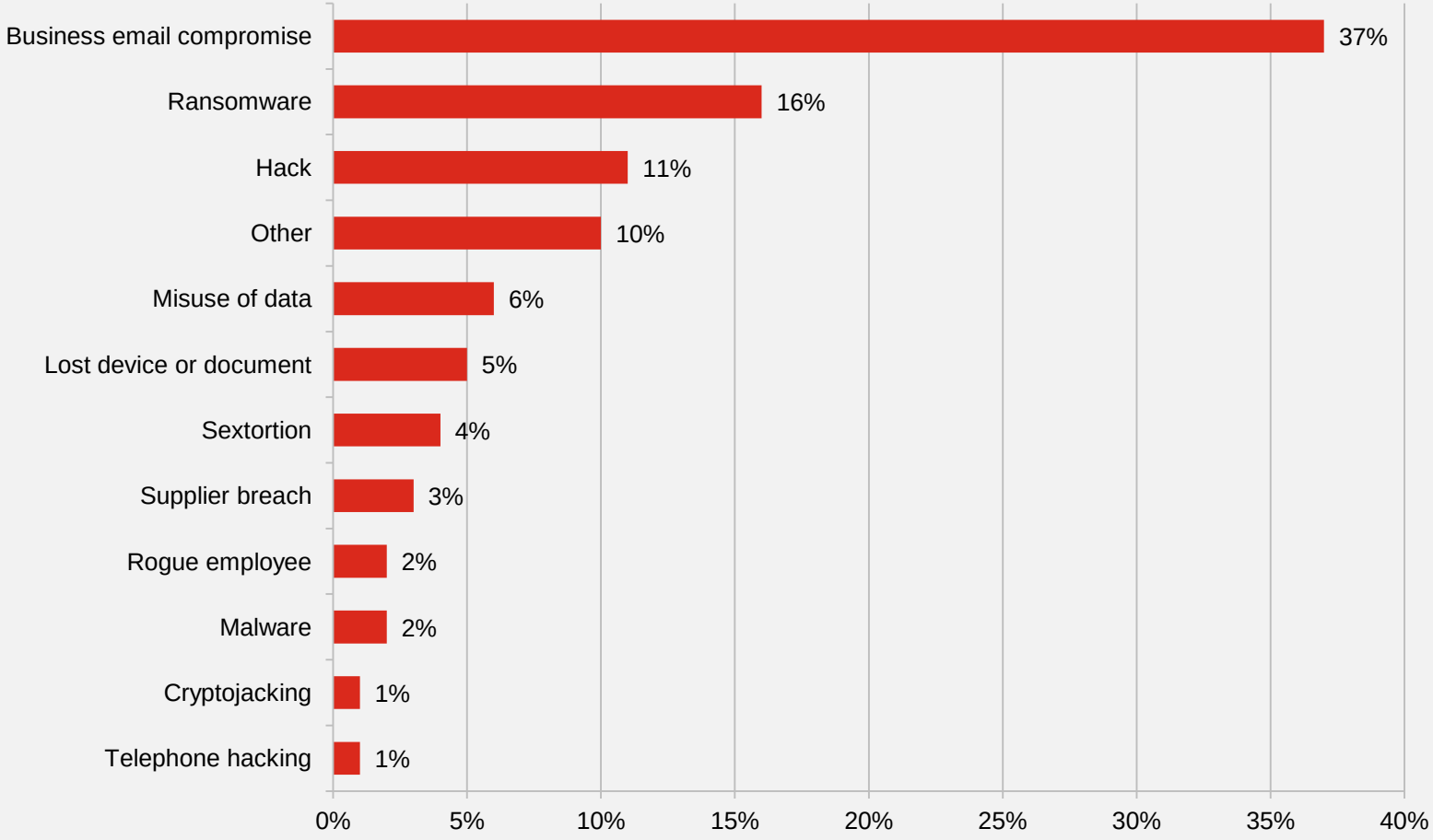
Through your email, I uploaded malicious code to your operation system. I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the internet resources. You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit. I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!) I made screenshot with using my program from your camera of your device. After that, I combined them to the content of the currently viewed site. There will be laughter when I send these photos to your contacts! BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence. I think $879 is an acceptable price.

# Cyber claims in 2018

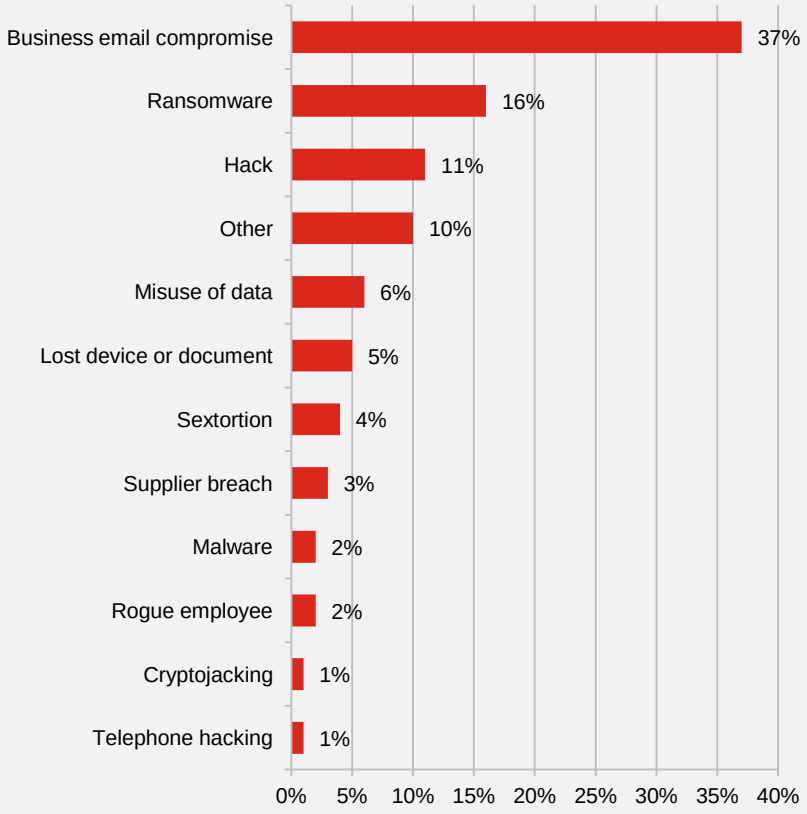
HISCOX
CYBERCLEAR®



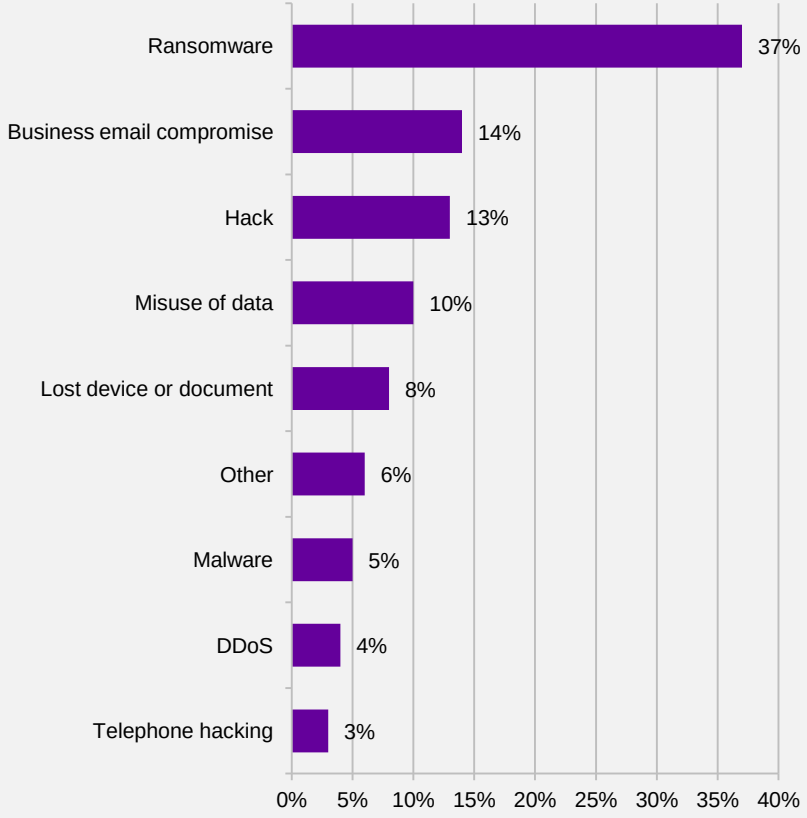
# How does that compare to 2017?

HISCOX CYBERCLEAR®

2018




2017



# Case studies - extortion

# The ‘good guy’
## First communication

HISCOX
CYBERCLEAR®

From: Dave

To: MrX@hiscoxinsured.com

Subject: Mr X, please add me to your LinkedIn network

Hello Mr X,

I am software developer and pentester. I searched for data leak. I found a lot of your files like financial statements, utility bills, driving licences, passports.

I want to report it. I am the good guy!
Dave

# The ‘good guy’
## Second round

From: Dave
To: MrX@hiscoxinsured.com
Subject: Data leak

Mr X,

Let me start from the beginning. I was looking for web servers with directory indexing enabled. I found one of yours: http://123456. As you can see, I found a lot of interesting files: [Lists files]

I have 37 screenshots to confirm it. Do you want me to send them to you?

I am the good guy. I want to report this leakage to you and collect bounty.
I can also sign NDA.

Best regards

Dave

# The ‘good guy’
## What had been accessed?

HISCOX
CYBERCLEAR®

- 44,000 data subjects
- All of which involved personally identifiable information (home and email addresses, telephone numbers, dates of birth etc.)
- 3,500 of which involved sensitive documents (passports, utility bills, bank statements etc.)

# The ‘good guy’
## What now?

HISCOX
CYBERCLEAR®

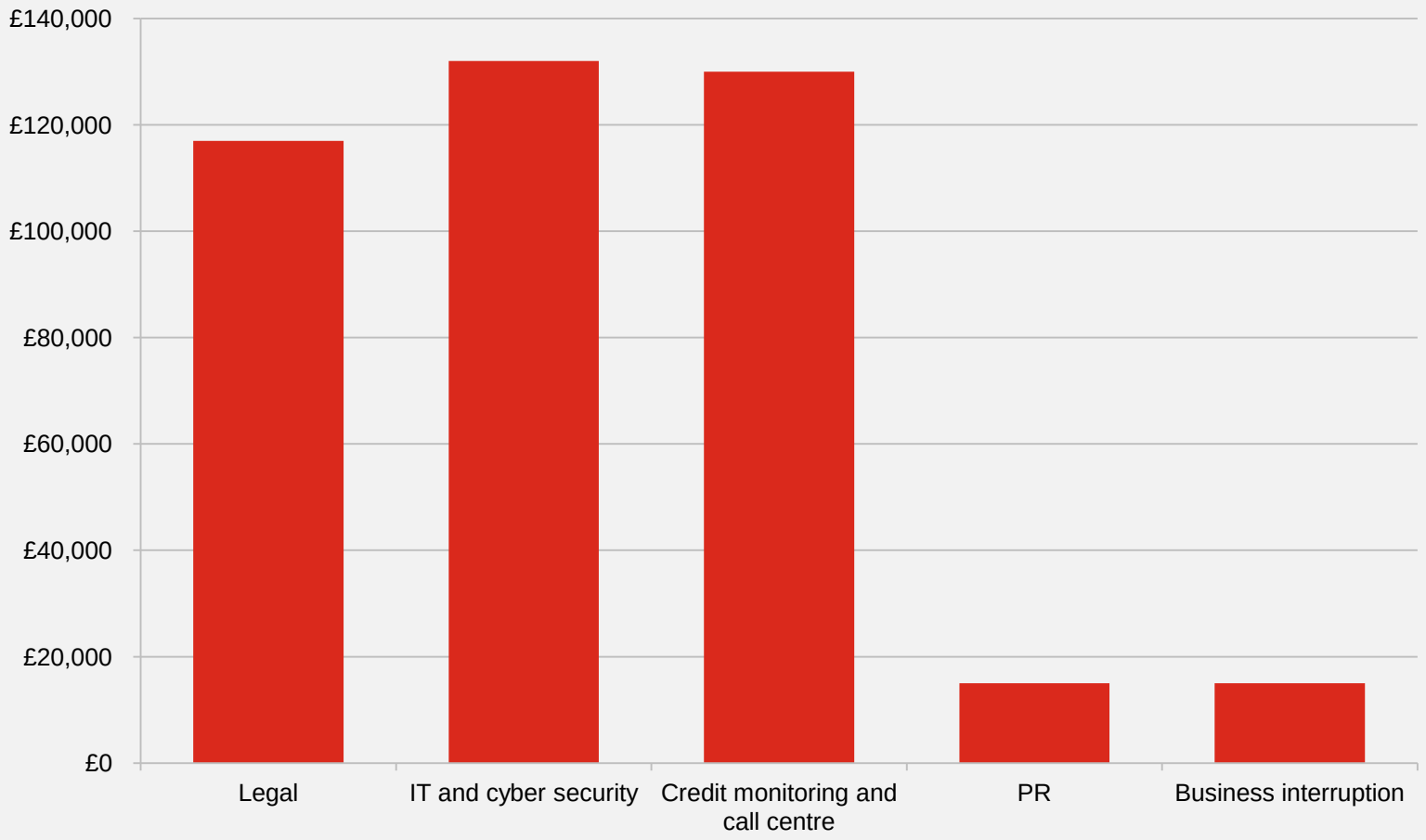
- Day one
  - 18.35. Insured contacted Hiscox 24/7 response line
  - 20.30. Call between Hiscox and cyber security consultants
- Day two
  - 09.30. Meeting at insured’s offices attended by Hiscox, cyber security consultants and insured’s breach response team (CEO, CFO, CIO and GC)
  - 16.00. Conference call with core team, now including external legal counsel

# The ‘good guy’
## Multiple workstreams

HISCOX
CYBERCLEAR®

1. Forensic investigation including ongoing dialogue with the hacker
2. ICO notification
3. Data subject notification: credit monitoring offered and call centre set up to deal with data subject queries
4. Dialogue with media and PR consultants

# The ‘good guy’
## What did it cost?



# Lockdown
## First communication

# Lockdown
## What was the impact?

- Servers encrypted
- 80% of insured's customers without one or more of email,  desktops or telephony
- Some insured data encrypted too

# Lockdown
## Day one – experts engaged

HISCOX
CYBERCLEAR®

- ✓ **Cyber extortion** – who is the attacker? Is paying ransom an option?
- ✓ **IT forensic** – how serious is the infection? Has data been stolen?
- ✓ **Legal** – do we need to notify ICO? What could customer claims look like?
- ✓ **PR** – what can we say to customers?

# Lockdown
## Day two – workstream updates

HISCOX
CYBERCLEAR®

- ✓ **Cyber extortion** – ongoing dialogue with attacker
- ✓ **IT forensic** – ransomware analysis. Customers now back online
- ✓ **Legal** – preparing ICO notification
- ✓ **PR** – twice-daily communications to customers. FAQs prepared

# Lockdown
## Week two – final steps

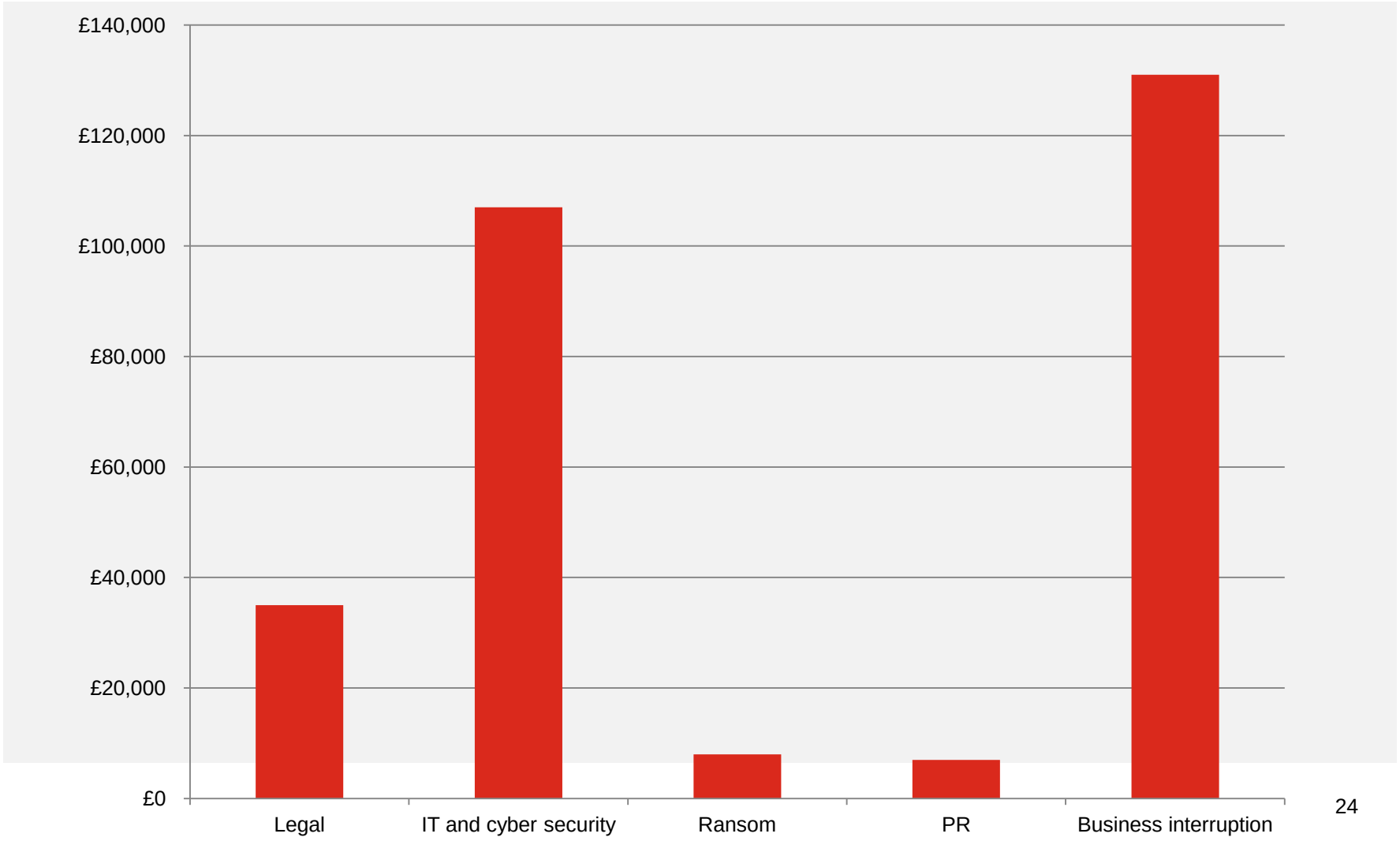
- ✓ **IT forensic** – concluding investigations
- ✓ **Insured** – monthly billing is due
- ✓ **Legal** – awaiting ICO response, addressing customer compensation claims
- ✓ **PR** – positive messaging. Focus on restoring insured's reputation

# Lockdown
## Week three onwards

HISCOX
CYBERCLEAR®

- ✓ **ICO** – ongoing dialogue
- ✓ **Customer base** – rebuilding the relationship
- ✓ **Business interruption** – some customers gave notice to terminate contracts

# Lockdown
## What did it cost?



# Case studies - theft

# Business email compromise
## How do the hackers look to exploit?

HISCOX
CYBERCLEAR®

- Insured received a payment in error from one of their customers
- Hackers had compromised the mailbox of the insured's customer, and advised the insured of a change of bank details
- Insured 'refunded' the amount, but to the criminals' account
- Constantly shifting dynamic can lead to potential coverage issues
- Spotted quickly enough, so funds recovered
- Still a significant amount of stress and disruption

# Not just an issue for businesses
## Individuals (particularly HNW) also at risk

HISCOX
CYBERCLEAR®

- HNW customer had recently sold business, and was purchasing a new home
- Due to business sale, was a cash buyer
- On day of completion, solicitor reminded customer that final requirement was transfer of funds
- Customer had already transferred the money, two weeks previously
- Transpired that email account compromised, and criminal inserted themselves in the middle
- Due to time lag in spotting, money had already been spread across numerous accounts globally, and was irrecoverable

# Fraud against cyber policies

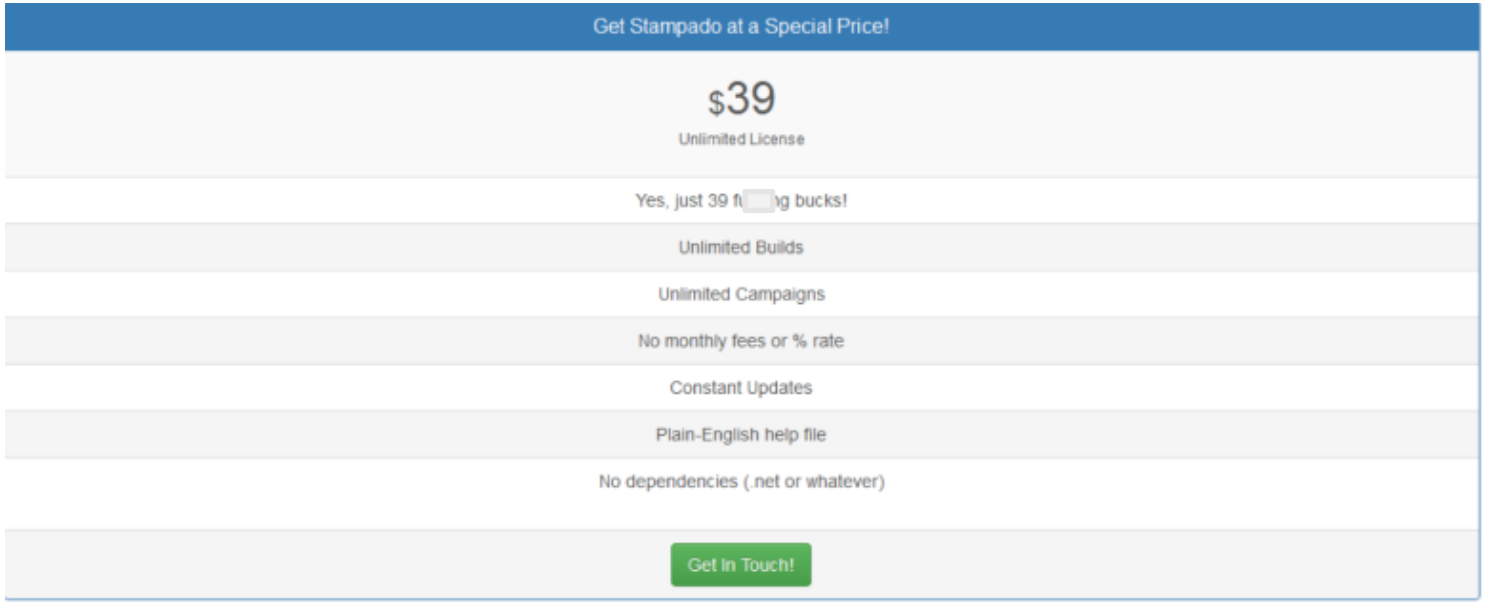
# Fraud against cyber policies
## A blindspot for the industry?

HISCOX
CYBERCLEAR®

- No examples within Hiscox:
  - Because it's not happening, or because spotting is difficult?

- Insurance fraud has been around as long as insurance policies have – no reason to think that cyber will be any different

- Easy to get hold of and deploy cyber attacks:



# Fraud against cyber policies
## Nature of policy response provides some protection

HISCOX
CYBERCLEAR®

- Generally, IT forensics engaged as part of claim response
- Full analysis of logs of what happened when, and by whom
- We make use of threat intelligence, particularly around ransomware, and will only make payment where we can be certain of ‘legitimacy’ of hackers
- Not infallible:
  - Company may not keep full logs
  - Particularly savvy fraudsters may be able to sufficiently cover their tracks
  - As fraud has been, to date, undetected, knowing what to look for is a challenge

HISCOX

Questions?