



MACQUARIE
BANK

Information Security

May 2019

Introductions

With you today is...



Michael Reynolds

Chief Information Security Officer
Banking and Financial Services (BFS)



Scott Schwartz

Information Security Manager
Banking and Financial Services (BFS)

Information Security...

It's a challenge for everyone.



Government



Business



Individuals



Government



“

We must not and will not wait for a catastrophic cyber incident before **we act to prevent future attacks.**

Malcolm Turnbull, Former Prime Minister of Australia
January 2017



Business



“

I don't know that much about cyber, but I do think that it's the **number one problem with mankind.**

Warren Buffett, Berkshire Hathaway CEO
July 2017



Business

LandMark White data breach (2019)



LMW last month entered an indefinite trading halt while it assessed the impact of the data breach, which led to client data being posted on a darkweb forum.



Business

LandMark White data breach (2019)



LandMark White's chief executive officer has left the property valuation firm after a decade and a half with the company.



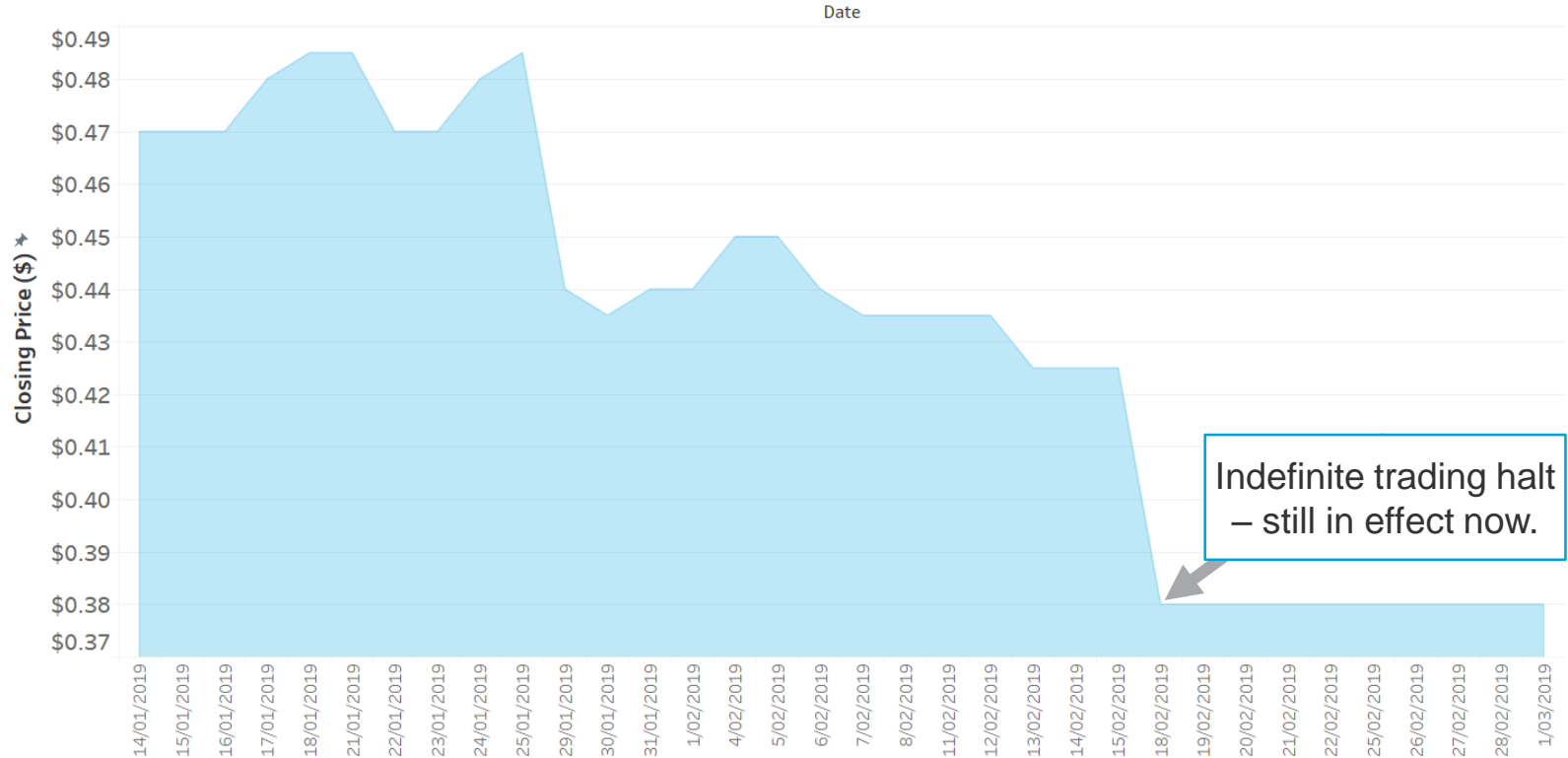
Business LandMark White data breach (2019)



Australia's major banks suspended their use of LMW in the wake of the breach.



Business LandMark White data breach (2019)



Indefinite trading halt
– still in effect now.



Individuals



“

When the hacking thing happened, it was so ***unbelievably violating*** that you can't even put it into words.

Jennifer Lawrence – Speaking about her 2014 iCloud Hack.
November 2017



Individuals



I lost some money to the internets.
This man from Telstra told me my
computer was infected with viruses.
I paid him to fix it but he lied.

Anonymous elderly citizen, actress' photo.
2018



“

What is the
threat
landscape?

Threats affecting business security

Security faces threats both inside and out of your business.



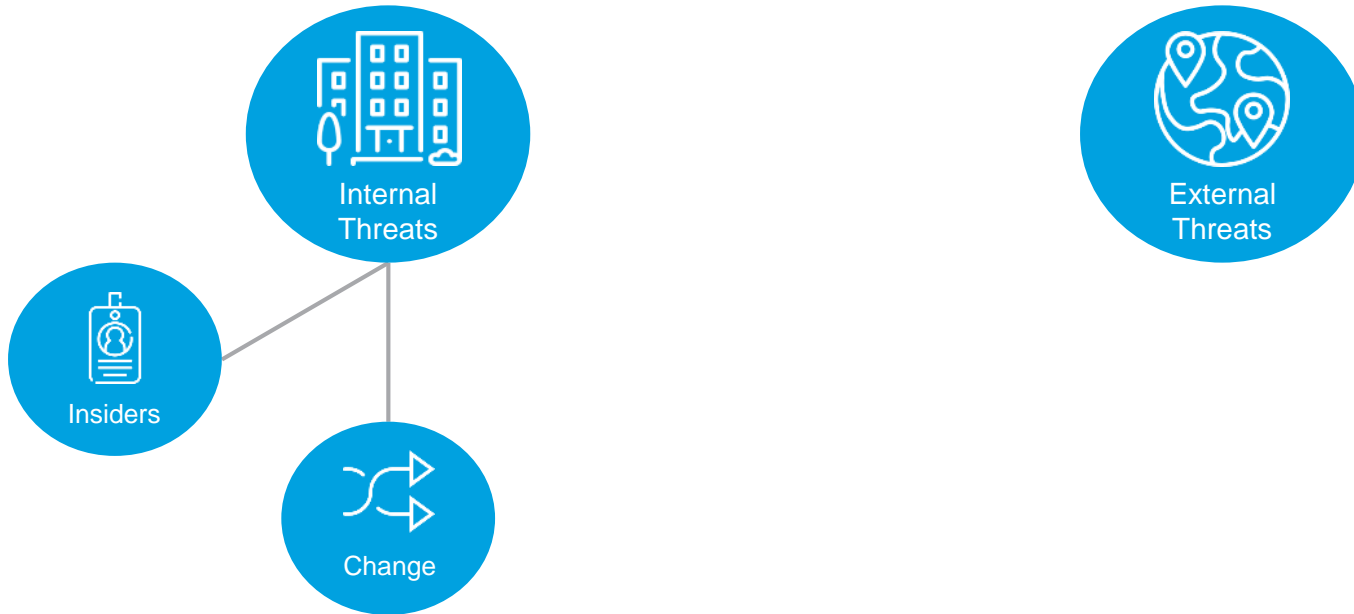
Threats affecting business security

Security faces threats both inside and out of your business.



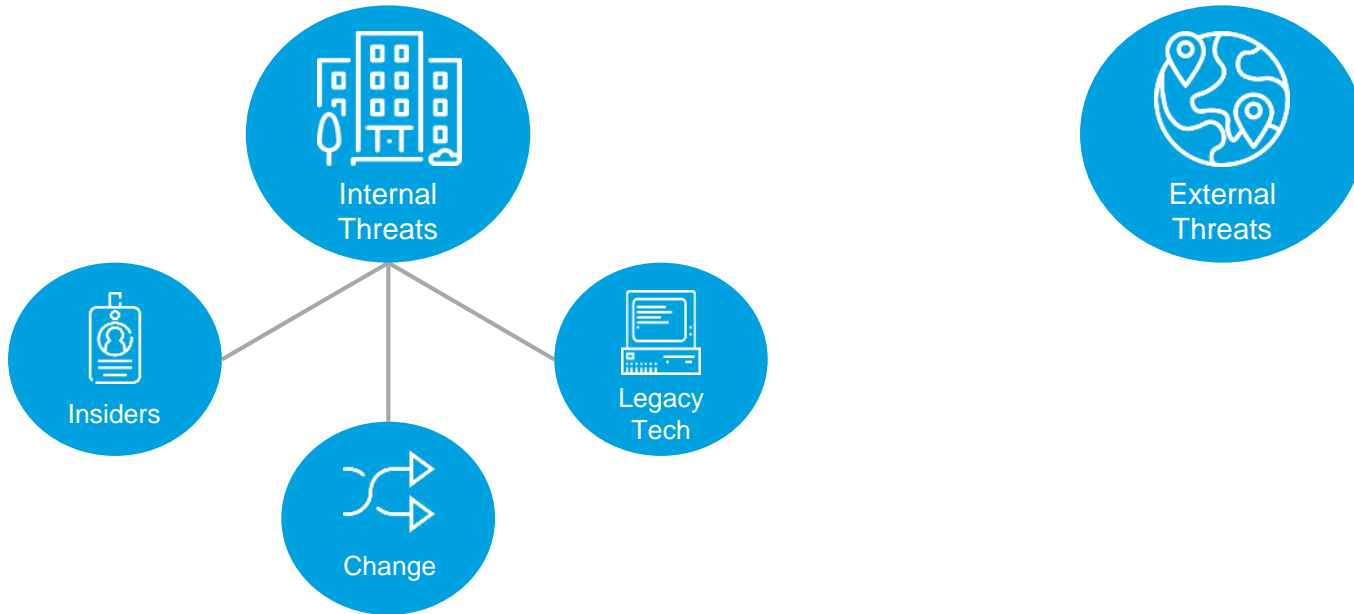
Threats affecting business security

Security faces threats both inside and out of your business.



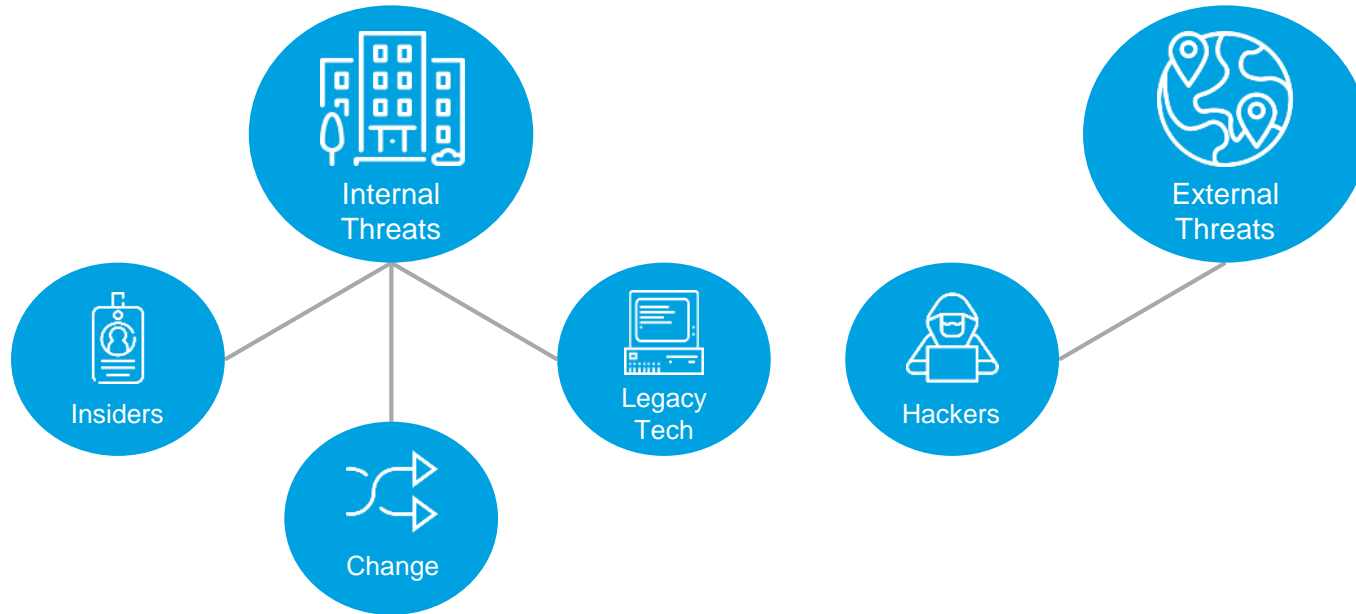
Threats affecting business security

Security faces threats both inside and out of your business.



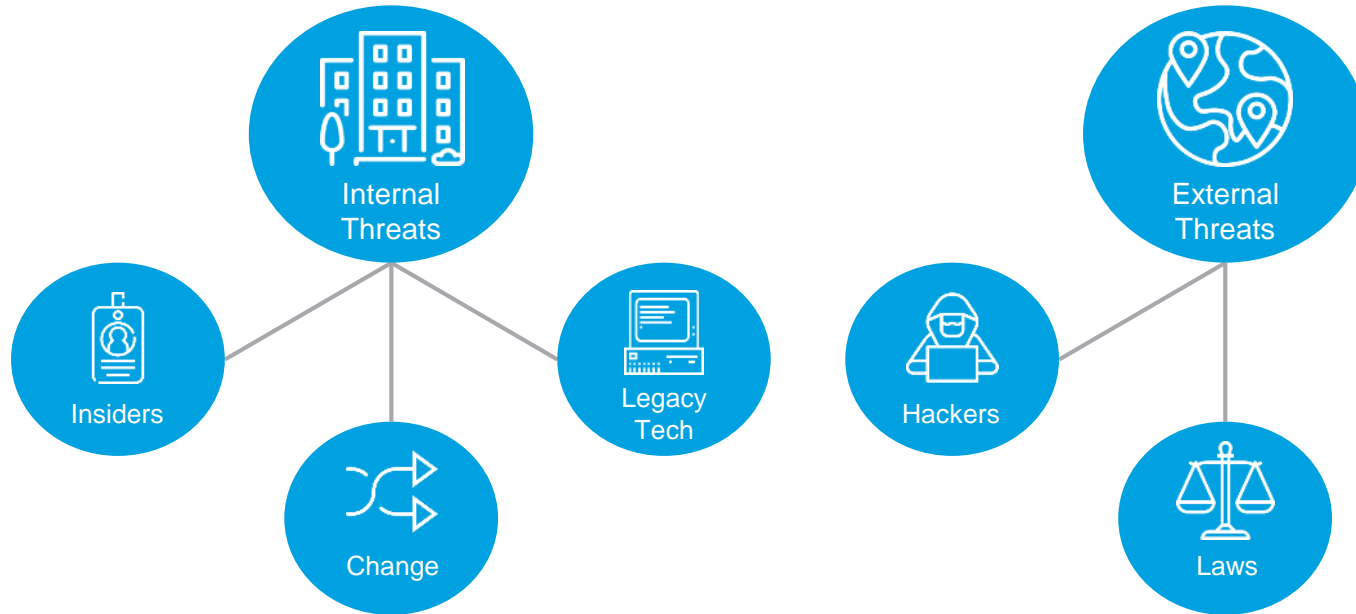
Threats affecting business security

Security faces threats both inside and out of your business.



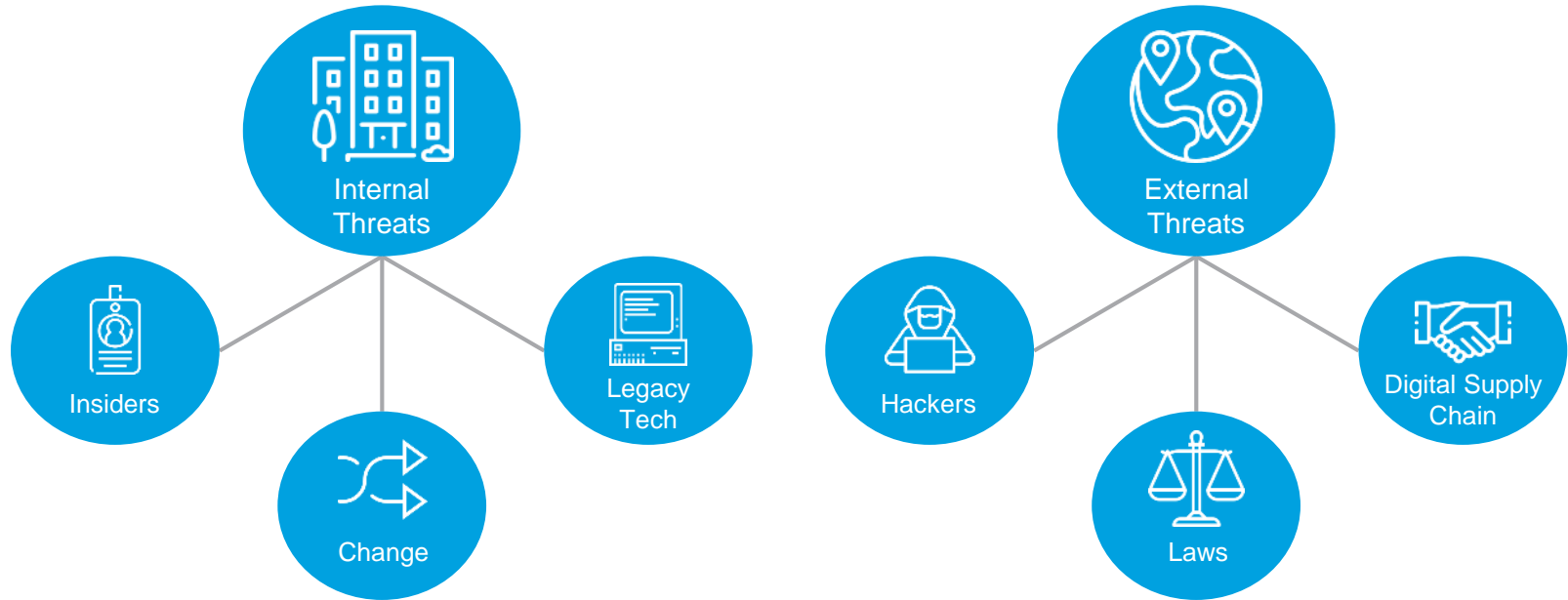
Threats affecting business security

Security faces threats both inside and out of your business.



Threats affecting business security

Security faces threats both inside and out of your business.



Why are medium sized businesses a target?

**Private
Investors**



Too small

**Banks and
Big Corporations**



Too big

**Medium sized
businesses**



Just right.



“

Who is
attacking us?

Where are we being attacked from?

Attacks come from everywhere but there are countries worse than others.



Origin

By volume, based on current attribution. Top 12 countries. Jul – Sept 2018.

Source: Akamai



When you think of a
hacker, you probably
think of this?



Who is attacking us?

The four most common hacker types and their motivation?

**SCRIPT
KIDDIES**



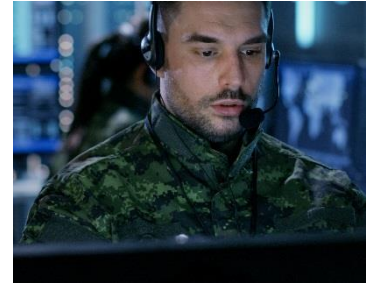
HACKTIVIST



**ORGANISED
CRIME**



**STATE
SPONSORED**



Increasing resources and sophistication

Who is attacking us?

Hackers are not who you'd think, and come from a wide variety of backgrounds.

How long have you been hacking?

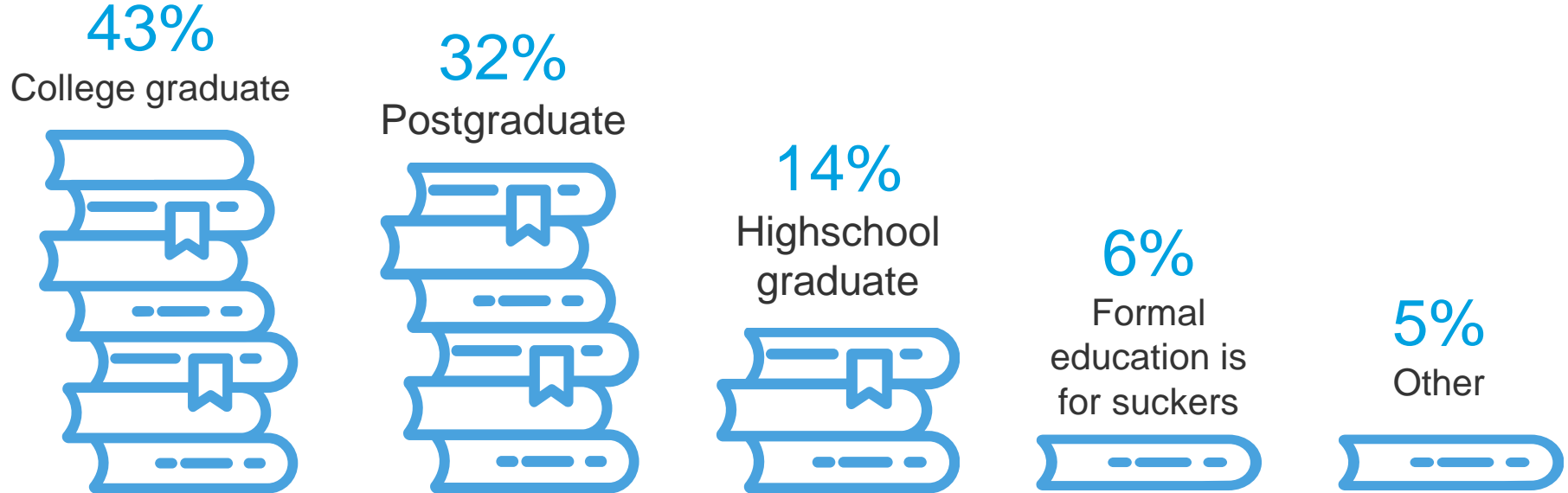
1-3 years	10%
4-6 years	19%
7-10 years	16%
11-13 years	10%
14-17 years	9%
17+ years	15%



Who is attacking us?

Hackers are not who you'd think, and come from a wide variety of backgrounds.

What is your highest level of traditions education?



Who is attacking us?

Hackers are not who you'd think, and come from a wide variety of backgrounds.

Why do you hack?



86%

I like the
challenge –
I hack to learn



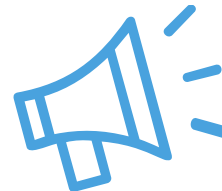
35%

I hack for
the lulz



21%

I hack for
financial gain



6%

I hack for social
or political moves



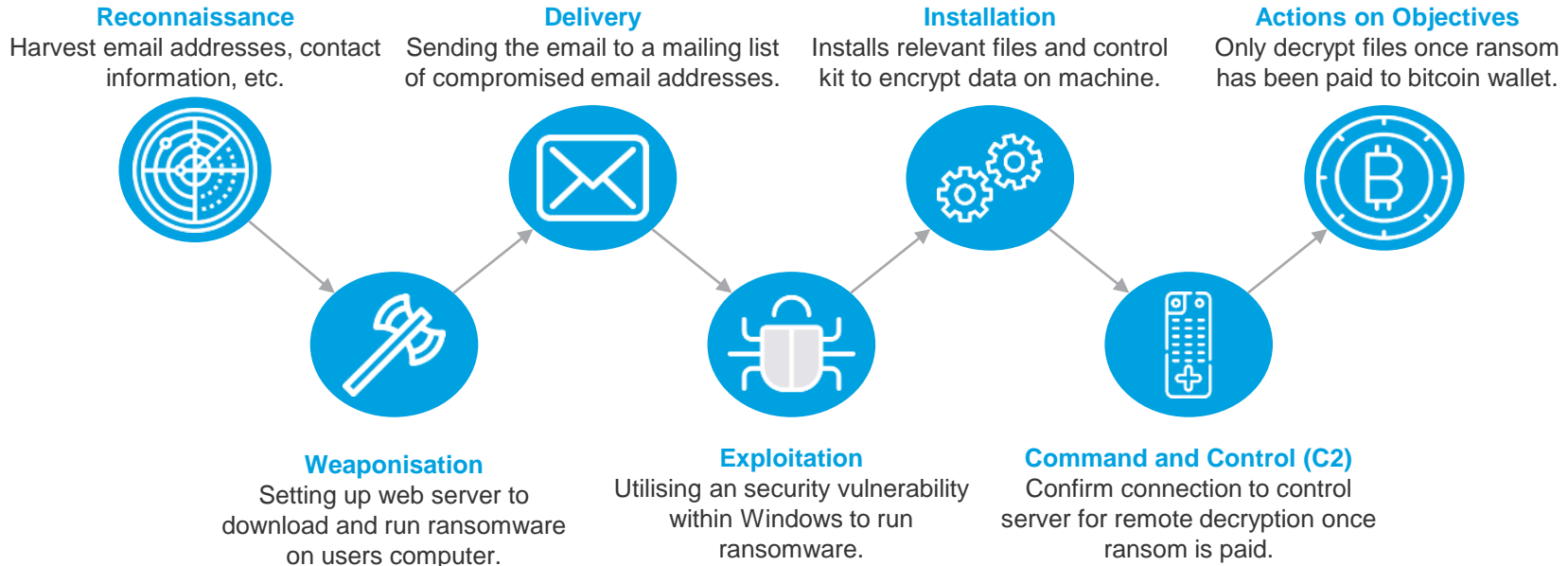
“

How are they
attacking us?

How are they doing it?

Hackers chain exploit and attacks together to target an organisation.
In Security communities, this is known as the “Cyber Kill Chain”.

Example of a Ransomware Kill Chain



How are they doing it?

Hackers use and combine many different vectors to attack a company, ranging from simple to the most complicated.



Phishing,
“Sms-ishing”
and Extortion



Email
Compromise



Malware



Ransomware



Supply Chain
Attacks

Phishing, “SMS-ishing” and Extortion

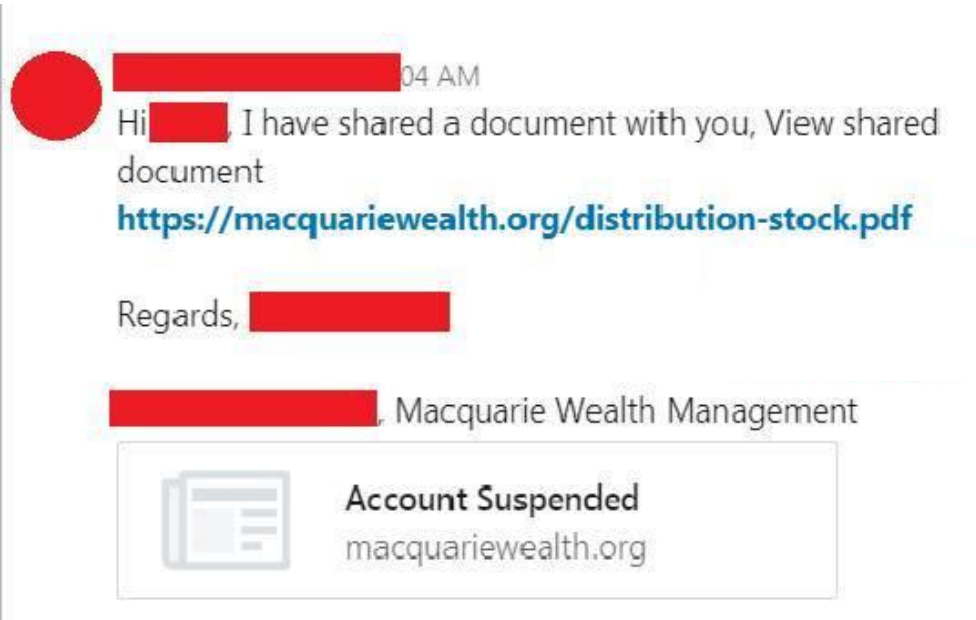
The easiest way to get something done. Ask nicely and convincingly.



Phishing

Phishing comes in all forms, such as sending messages on social media.

Compromised LinkedIn account sending phishing messages to their network.



Phishing

Phishing is most common via emails.

RE: Busieness proposal – respond fast.

1 minute ago at 5:39 pm

From



[Hide](#)

To



John,

You shall send deposit for distributions and shippings of to the following western unions bank:

SWIFT Code: 1293513513143

Bank: First Bank of Nigeria

Address: Noah Ave, Jos, Nigeria

Name: Chan Eionw

IBAN: 1829351241

Pleas pay fast – I do not have much time left.

Solomon

Eticket 9632-36

6 days ago at 2:02 am

From [Qatar Airways](#) >

[Hide](#)

To [REDACTED]

Reply-To [Qatar Airways](#) >

[View in browser](#)



Thank you for booking with Qatar Airways
We have received your booking under reference [9632-36](#)

Yours sincerely,
Qatar Airways

You can also view the details of this request by following this link:
<https://www.qatarairways.com/?request=9632-36>

* Terms and conditions apply

Qatar Airways Tower 2, Airport Road, PO Box 22550, Doha, Qatar

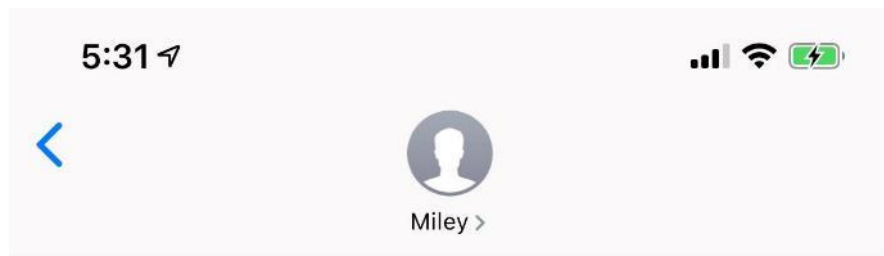
You are receiving travel offers for flights departing from as it is selected as your preferred country of departure. If you would like to change your country of departure or change the frequency of the emails you receive, you can [modify your preferences](#). To stop receiving offers from Qatar Airways, [click here to unsubscribe](#).

* For [terms and conditions](#) of our current promotion and special offers, visit the [Qatar Airways website](#).

All rights reserved. © 2019 Qatar Airways. Going places together.

SMS-ishing

Putting a phish right into your hand with fewer red flags to spot.



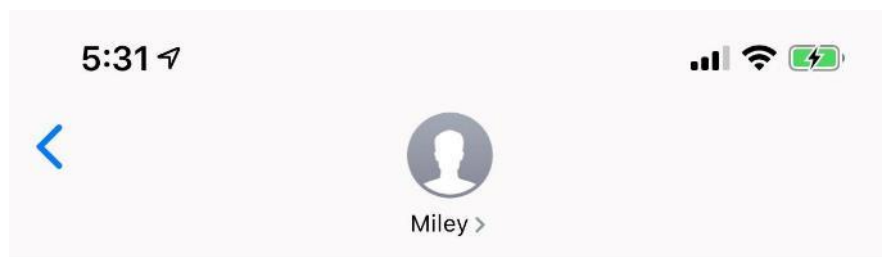
Text Message
Today 5:27 pm

We are looking for Mr Dumpty in
West Swan. It's regarding the
selection of your name. Read more
here: <http://cup.cab/3nis8>

SMS with a phishing link with
approximate location of target to
build trust.

SMS-ishing

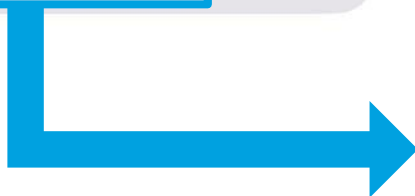
Putting a phish right into your hand with fewer red flags to spot.



Link **redirects** to a Coles site asking for your details to redeem a “gift”... in French.

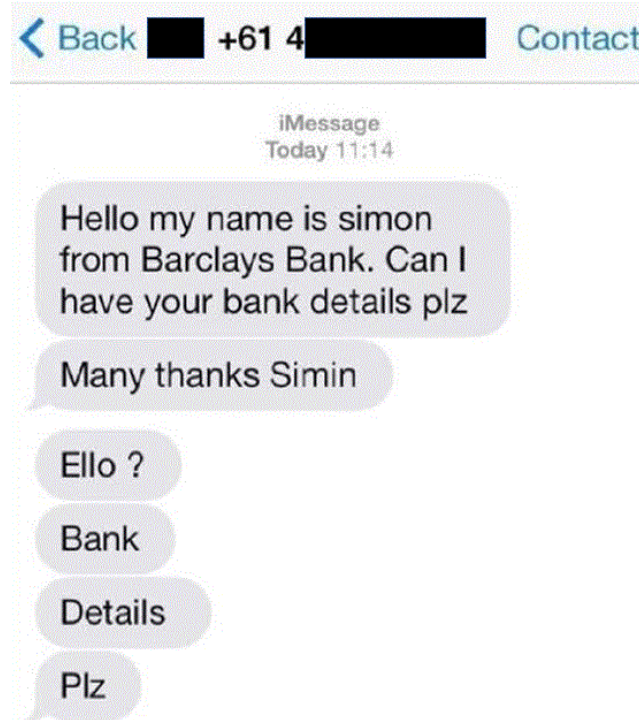
Text Message
Today 5:27 pm

We are looking for Mr Dumpty in **West Swan**. It's regarding the selection of your name. Read more here: <http://cup.cab/3nis8>



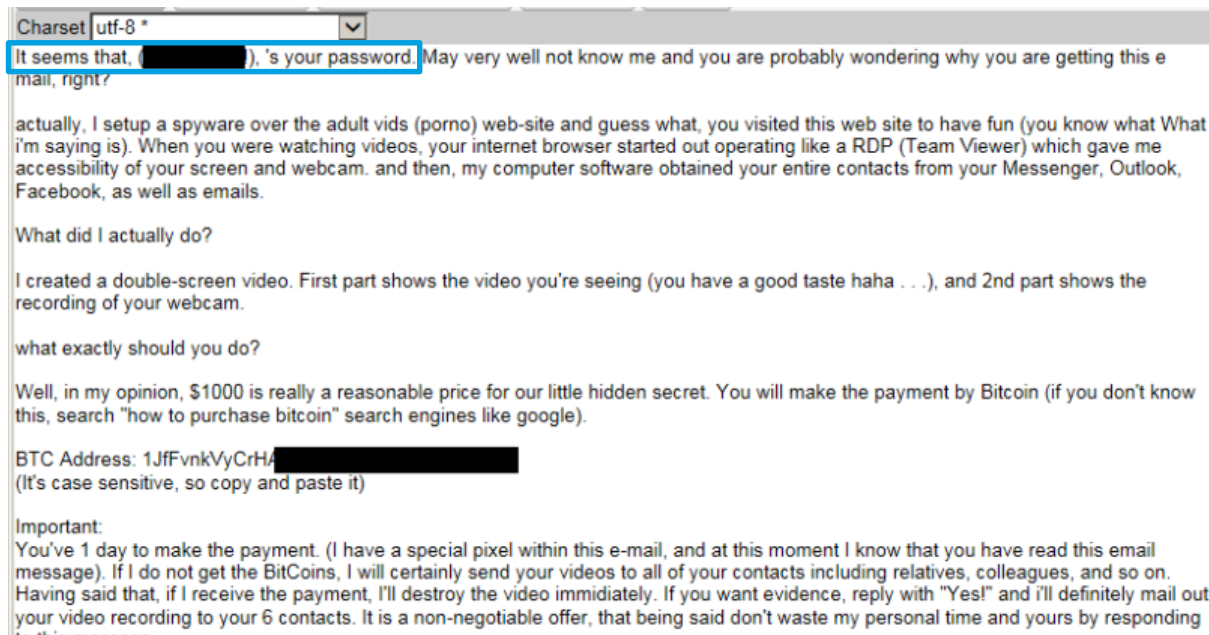
SMS-ishing

SMS-ishing can also be downright dumb sometimes though.



Extortion Phishing

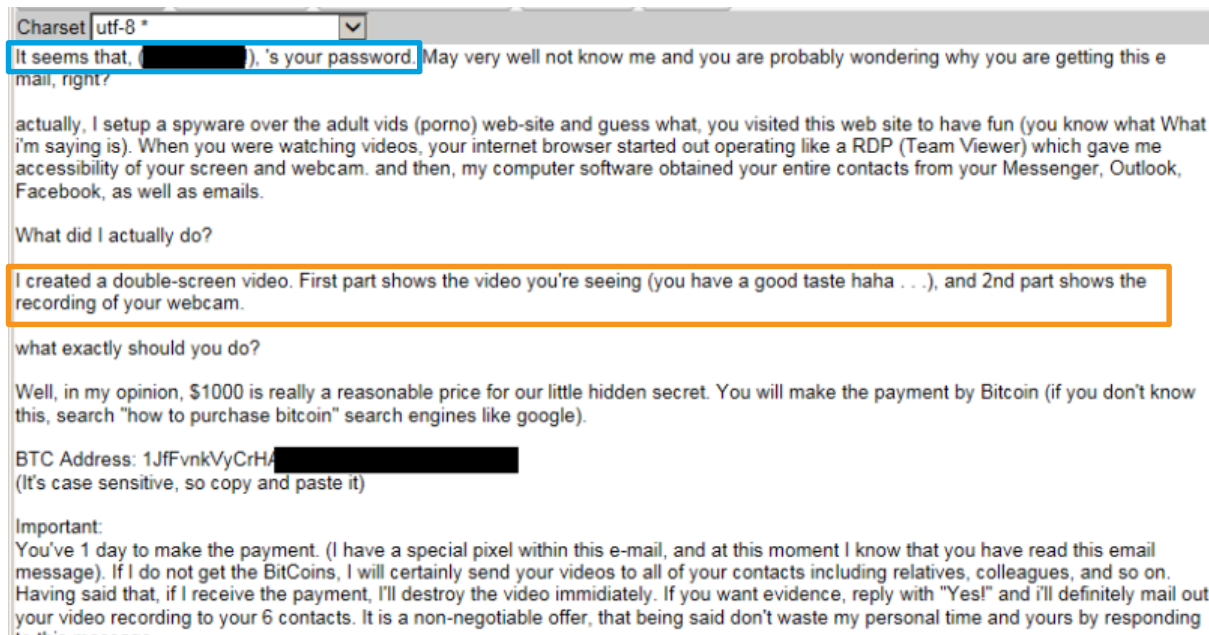
Creating panic to get action using your own breached credentials against you.



Phishing email
purporting to have the
users password.

Extortion Phishing

Creating panic to get action using your own breached credentials against you.

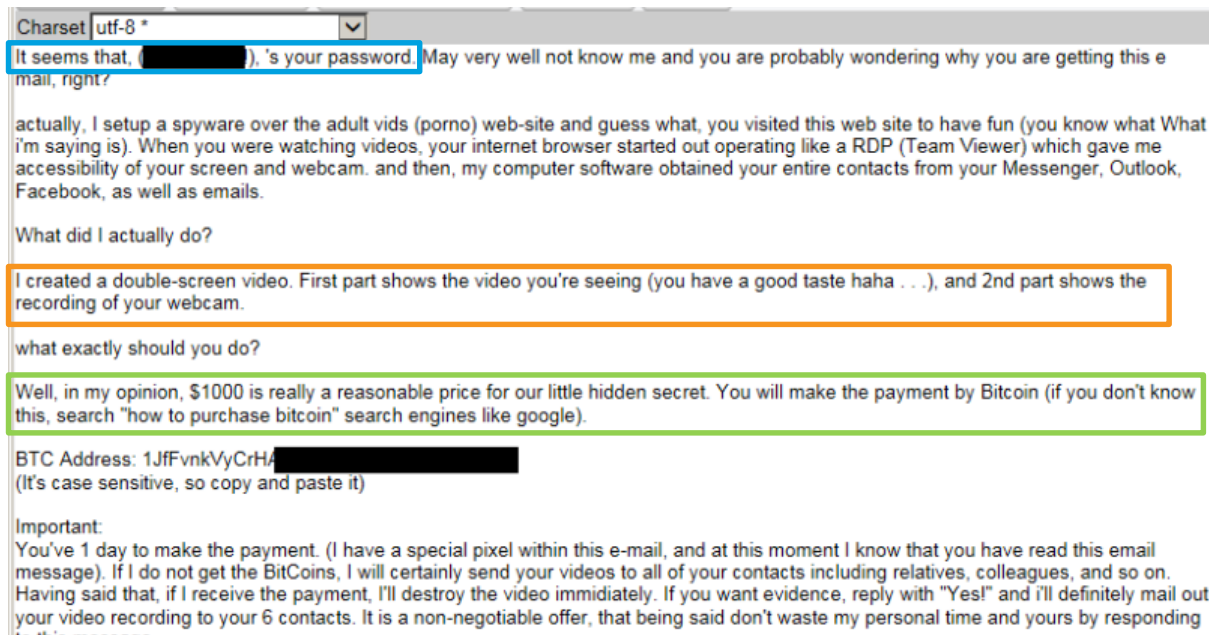


Phishing email
purporting to have the
users password.

Phisher threatens to
leak video of user
viewing adult content.

Extortion Phishing

Creating panic to get action using your own breached credentials against you.



Phishing email
purporting to have the
users password.

Phisher threatens to
leak video of user
viewing adult content.

Phisher demands a
ransom paid via
Bitcoin.

Email Compromise

Want to look convincing? Take over someone's digital identifier.



Email Compromise

Taking over an email account gives a wealth of information on a person, their business and their finances.

Subject: Transfer

Good Morning [redacted]
I hope everything is going well

I would like to make a transfer
instruction and send it back to [redacted]

Hi [redacted]

Yes it is genuine, prepare an instruction and send it to me to for confirmation.

Regards

On Mon, Jul 14, 2014 at 9:58 AM, [redacted] wrote:

Hi [redacted]

low. i need you to prepare the

With all the scamming going on lately, I just wanted to check that the request below is genuine.

Can you please confirm?

Email Compromise

What would happen if your vendor was compromised and requested a change to their bank account details?

G.S.T.	\$	218.04
Total this invoice (inclusive GST)	\$	2,398.40

Amount due before 01.11.2017

Please pay on Invoice. No Statement issued.

PAYMENT OPTIONS

By Direct Deposit to the following Bank Account:

Reference details: (NOTE: Ensure this reference is included with your payment)

BSB: 062-231

Account: 10188188

Bank/Branch: CBA/Redfern NSW

cut along dotted line

Payment can be made by Visa / Mastercard / Amex by completing the details below and returning this tear-off slip to our office at the address shown above.

NOTE: Payment more than \$5,000 will incur a card fee. VISA/MasterCard 1% | AMEX 2%

Card type (Circle one): Visa / Mastercard / Amex

Card number: _____

Inv.Ref:

Expiry: ____ / ____

CCV: ____

Amount: \$ 2,398.40

Name Shown on Card:

Signature:

No claims in respect of this invoice will be recognised unless made within 7 days.

Email Compromise

Smart hackers will use what they find in your email inbox to add legitimacy to their scams. Some don't do it as well as others.

Subject: RE: Urgent Transfer

Subject: RE: Urgent Transfer

y,Can you

I have malaria fever,can you please complete the transfer by 10am?thank you a lot

sent from my iPad

Thanks in advance,

Thanks in advance

sent from my iPad

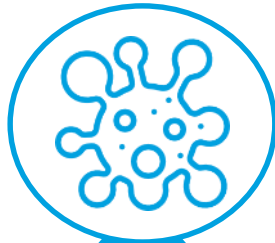
Malware

Nasty computer software with a long list of uses.



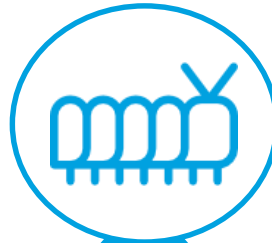
Malware

It's a catch all term for malicious computer software.



Viruses

Adware



Worms

Hijackers



Spyware

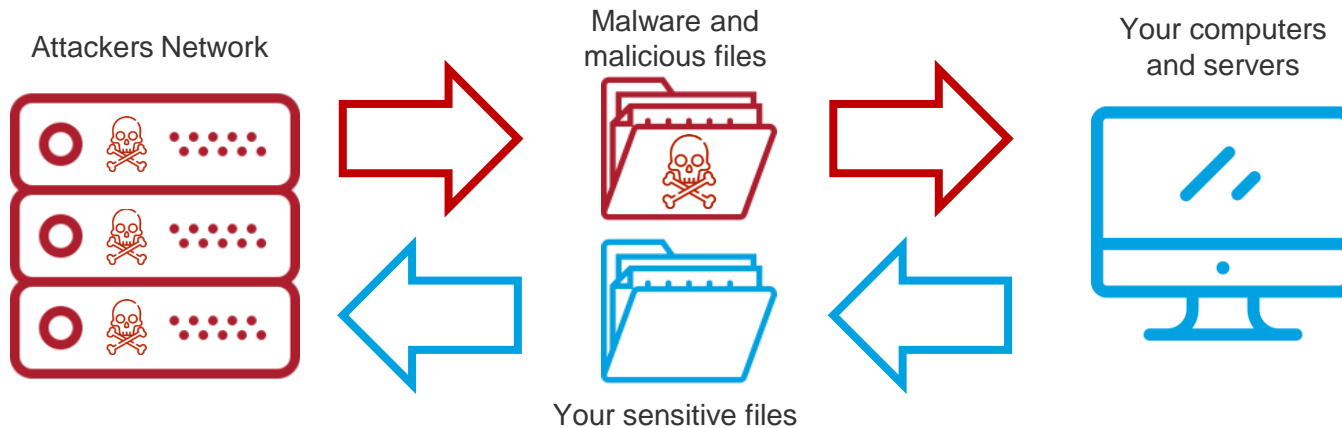
Trojans



Malware

What can it do?

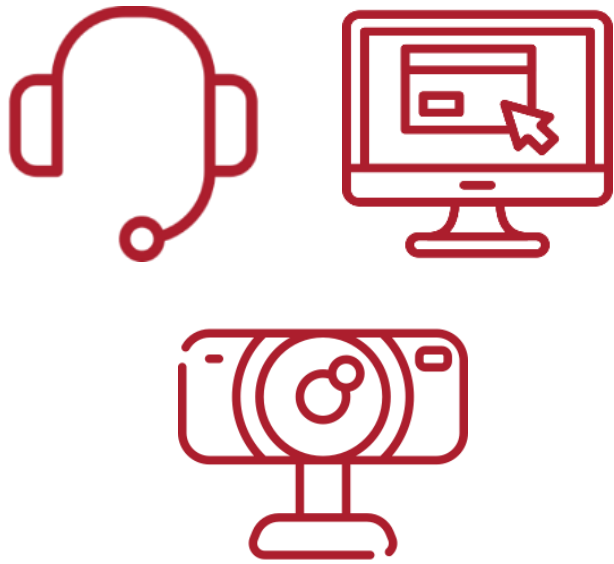
Download malicious software, files to your computer or steal your data.



Malware

What can it do?

Hand over your passwords and take control of your computer.



“Big Brother is
always watching
and listening.”

Ransomware

Pay or your data gets it.



Ransomware

Pay or your data gets it.



Ransomware

The things we learnt from calling a ransomware helpline

#1 – They don't normally negotiate

6

USD433 is like EUR400 - that is monthly salary in our country - 200 for housing, 100 for food, 100 for childrens Im poor for this kind of extortion... :-(do You have conscience to do it ? please send Me the decryption tool please please... :-(

6

Slovakia is poor for most people here... :-(

Support

Sir, sorry, but no discounts here. Your price is below 500 USD, but many people has more than 1000 USD, so your price is not so high.

Ransomware

The things we learnt from calling a ransomware helpline

#2 - ... except when Bitcoin rates move

6

Hi sir, I transferred the bitcoins as per amount stated, but when I refill the complete amount from my wallet, it is slightly below, and insufficient. I do not know why. I desperately need my files back for my exams. Please help give me discount for the remaining amount. Thank you.

6

I travelled all the way to the bitcoin exchange to verify and transfer the money. Please help. I cannot wait another day.

Support

We have added to your account a small amount of USD, so now you could make purchase.

In next time - use calculator on Payment Area.

Ransomware

The things we learnt from talking to a ransomware helpline

#3 – Customer service is important to them.

Support

Sir, you refilled your account with 66 dollars. Item Full restore is unavailable due to low funds.

D

Yes - was waiting for the remaining amount to come :)

Support

So.. we are patiently waiting.
Lets take a cup of coffee now.

Support

How are you?

D

Well - I did not plan on spending my day with this haha

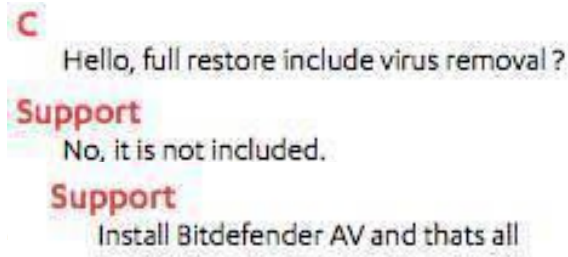
Support

As some person said:
We can not predict what will happen to us tomorrow. So lets enjoy the moment.
I invite you to enjoy, even unpleasant - but unusual situation in your life.
And coffee will make you a good company, while your Time will be restoring.

Ransomware

The things we learnt from talking to a ransomware helpline

#4 – Oddly, they recommend installing anti-virus



A screenshot of a chat conversation with a ransomware helpline. The chat is displayed in a dark-themed window. The user, labeled 'C' in a red bubble, asks: "Hello, full restore include virus removal?". The support agent, labeled 'Support' in a red bubble, responds: "No, it is not included." The user then asks another question, and the support agent responds: "Install Bitdefender AV and thats all".

C
Hello, full restore include virus removal ?

Support
No, it is not included.

Support
Install Bitdefender AV and thats all

Supply Chain Attacks

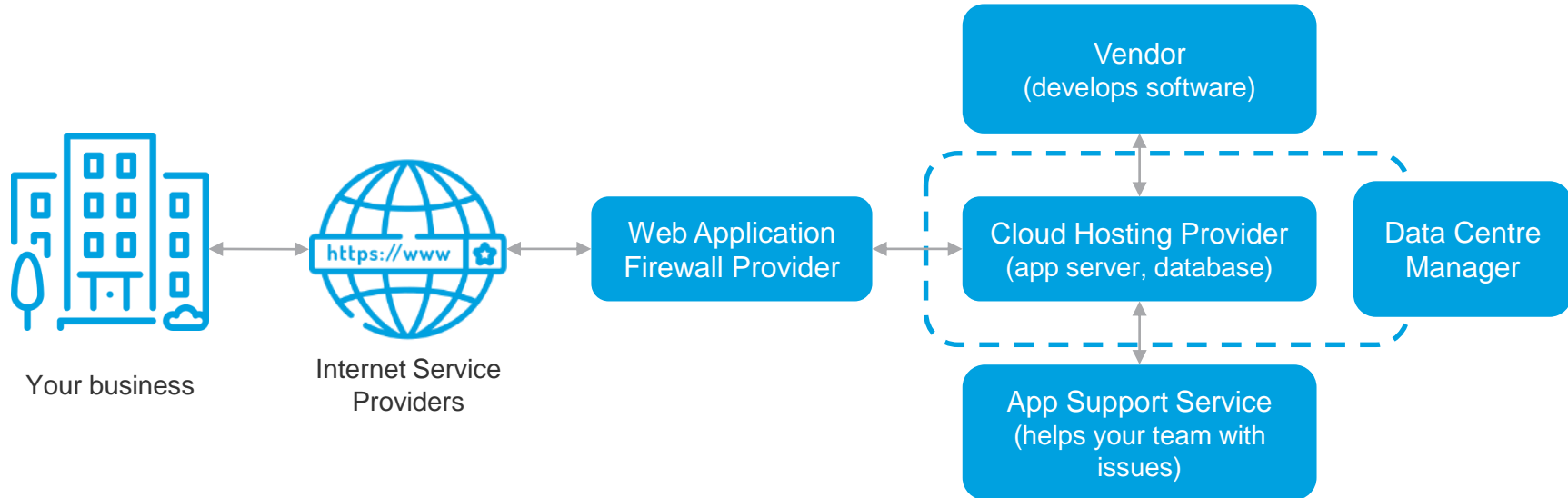
If we can't get you directly, let's use your third parties.



Supply Chain Attacks

Technology doesn't just stop at the walls of your office.
Using third parties adds additional risks to your organisation.

Typical setup of a Software-as-a-Service (SaaS) offering





“

**How can you
build a cyber
smart business?**

1

Remember, bad actors
are everywhere.



2

Get your people set up for success

General Staff



Build Awareness

Technology Staff



Train on Security

Security Staff



Get Certified in
Security

3

Define your risk appetite and align your investment to a framework.



4

Invest in securing crown jewels,
not just everything.



5

Be sceptical. Don't take
everything on face value.



The background of the slide is a dark blue gradient. It is filled with a dense pattern of light blue binary code (0s and 1s) and various numbers (0-9) in a similar light blue color. The numbers and binary code are scattered across the entire background, creating a digital or data-themed aesthetic.

Questions?
Thank you.