

The Baker McKenzie logo is positioned in the top left corner. It features the company name in a white, sans-serif font. The word "Baker" is on the top line, and "McKenzie." is on the bottom line. The text is set against a dark, semi-transparent rectangular background that has a slight gradient and is partially overlaid by the abstract geometric shapes of the slide's background.

**Baker  
McKenzie.**

# Cybersecurity – current trends and what's next

Paul Glass, Stephen Reynolds | Tuesday 9 November 2021



# Speakers



**Paul Glass**  
Partner



**Stephen Reynolds**  
Partner



# Agenda

1

INTRO TO CYBERSERURITY

---

2

TRENDING CYBER ATTACKS

---

3

HOW TO PREVENT

---

4

COMPLIANCE

---

5

QUESTIONS

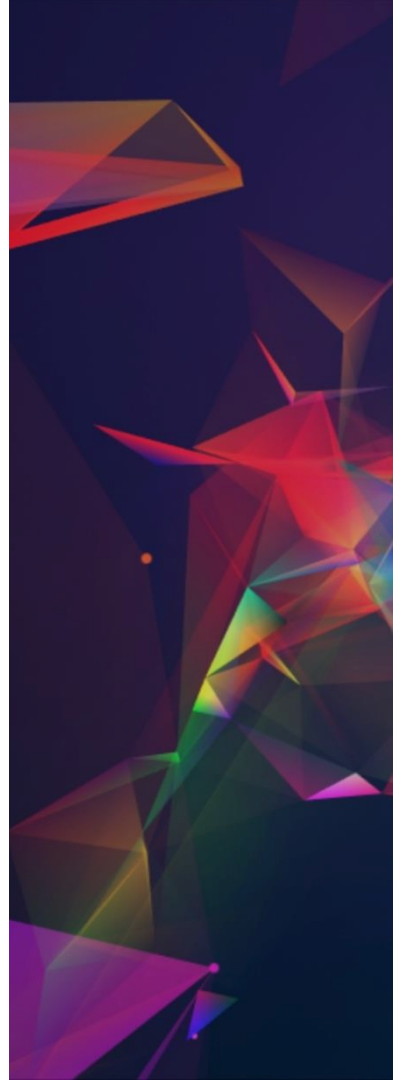
---



1

# Intro to Cybersecurity

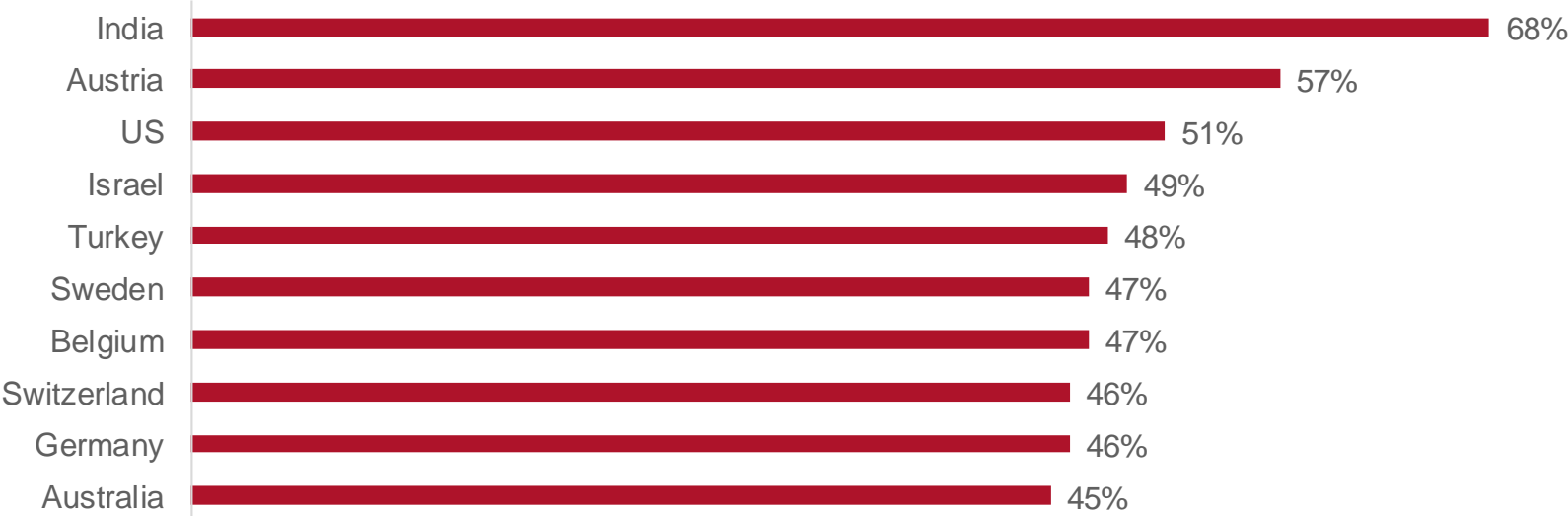
# Why Should You Care?





# Ransomware is a Global Issue

Share of Organizations, by Country, That Were Affected by Ransomware



Source: Statistica, <https://www.statista.com/statistics/1246438/ransomware-attacks-by-country/>

# Why Should You Care?



THE WHITE HOUSE  
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

## Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative meeting October 2021



Having gathered virtually on October 13 and 14 to discuss the escalating global security threat from ransomware, we the Ministers and Representatives of Australia, Brazil, Bulgaria, Canada, Czech Republic, the Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, Saudi Arabia, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates, the United Kingdom, and the United States, recognize that ransomware is an escalating global security threat with serious economic and security consequences.



The background features a complex, abstract geometric pattern of overlapping, semi-transparent polygons in shades of purple, blue, and red. In the upper right corner, there is a network of small, colorful dots connected by thin lines, resembling a data visualization or a molecular structure. The overall aesthetic is modern and digital.

2

# Trending Cyber Attacks



# Trending Cyber Attacks



***"Amateurs hack computers,  
professionals hack people."***

*- Some Hacker*

# Trending Cyber Attacks

## How are People Hacked?



Hackers try to trick people into...

- Running the hacker's malware
- Handing over credentials to the hacker
- Directly working for the hacker



# Trending Cyber Attacks

## Ransomware Example



**From:** Candidate, Joe <joe.candidate@gmail.com>  
**Sent:** Monday, September 15, 2015 10:58 AM  
**To:** <hrdirector@yourcompany.com>  
**Subject:** Open Position  
**Attachments:** Resume.pdf

Dear HR Director,

Please see my resume attached.

Thanks,

Joe

# Trending Cyber Attacks

## Ransomware Example



**From:**  
**Sent:**  
**To:**  
**Subject:**  
**Attachments:**

Dear HR Director,

Please see my request.

Thanks,

Joe

CryptoLocker

### Your personal files are encrypted!



Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

Private key will be destroyed on  
**9/15/2013**  
**8:44 PM**

Time left:  
**57 : 45 : 37**

Next >>

# Trending Cyber Attacks

## Another Ransomware Example



The image shows two overlapping screenshots. The background screenshot is a ransomware payment page with the following text:

- Buttons: Payment, Stolen data, Free decrypter
- Text: "Your files are encrypted. Only way to decrypt your files is by paying the ransom. Your user key: **2A1FFDFC**. The system is fully automated. After payment, your files will be decrypted."
- Section: "Invoice for payment" with a red "EXPIRED" stamp.
- Text: "You can buy the decrypter program for your network."
- Text: "Payment expired! New price: 2000000\$ (228.46700000 BTC)"
- Text: "Decrypter for: ALL NETWORK / ALL COMPUTERS / ALL DATA"
- Text: "Bitcoin address: **3DgQCQm527JES8Pj4xTAUSk56Lg2u**"

The foreground screenshot is a Google search for "228 bitcoin to usd". The search results show:

- Search query: 228 bitcoin to usd
- Results: About 3,830,000 results (0.48 seconds)
- Conversion: 228 Bitcoin equals 2,088,261.12 United States Dollar
- Chart: A line chart showing the price of Bitcoin in USD from June 30 to July 11. The price fluctuates between approximately 9,000 and 9,700 USD.
- Input fields: 228 Bitcoin, United States Dollar
- Disclaimer: Jul 20, 1:40 PM UTC - Disclaimer
- Source: Data provided by Morningstar for Currency and Coinbase for Cryptocurrency



Your files are encrypted.

--

Rebooting, shutting down will cause you to lose files without the possibility of recovery.

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help. The only way to get your files back is to cooperate with us and get the decrypter program. Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

We advise your organization to contact us as soon as possible, otherwise your files will be published online on 25 January 2022. To avoid publication and recover your files, pay the amount of EUR 10 million.

Contact us at: [xxxxxxxxx@tuta.li](mailto:xxxxxxxxx@tuta.li)

Don't forget to include your code in the email:

```
{code_8379f5b_i8jsb:wYYAaXJLOHSSifho26qph+XqlmWWWmoik9f+khUG987idho987BUbj9817h  
BIGulkj}
```

# Trending Cyber Attacks

## Current Ransomware Example

A screenshot of a ransomware payment page. The browser address bar shows 'lockbitsap' and '3ka4k2did.onion'. The page content includes the text 'TRIAL DEC', 'You can decrypt a single file', 'we can do it', 'ATTENTION', 'Decryption is available once for you', and 'two files of your choice and we will decrypt them free of charge. If we reach mutual'. A large white overlay with a red bar contains the text 'UNTIL FILES 1D 10:49:37 PUBLICATION' and a timestamp '07 Oct, 2021 03:17:00'.

← → ↻ lockbitsap 3ka4k2did.onion

TRIAL DEC

You can decrypt a single file  
we can do it

ATTENTION

Decryption is available once for you

two files of your choice and we will decrypt them free of charge. If we reach mutual

**UNTIL FILES**  
**1D 10:49:37**  
**PUBLICATION**

07 Oct, 2021 03:17:00

# Trending Cyber Attacks

## Triple extortion...



"Unfortunately, [your biggest customer's] security isn't as good as it should be. We've encrypted all of their data and systems, so you aren't going to be paid for your last deliveries any time soon. Sorry about that 😊

We also copied all their data. Don't worry, it's safe with us, for now. But if [customer] doesn't pay, we'll publish it. We found a lot of your data in there too. Unless you pay us 50BTC by [date], we'll publish your data too. You can contact us at [xxxxxxx]

The background features a complex, abstract geometric pattern of overlapping triangles in various colors including red, purple, blue, and green. The triangles are semi-transparent, creating a layered effect. In the upper right corner, there is a network of small, colorful dots connected by thin lines, resembling a molecular or data structure. The overall color palette is dark and vibrant, with a gradient from deep blue to black.

**3**

# How to Prevent

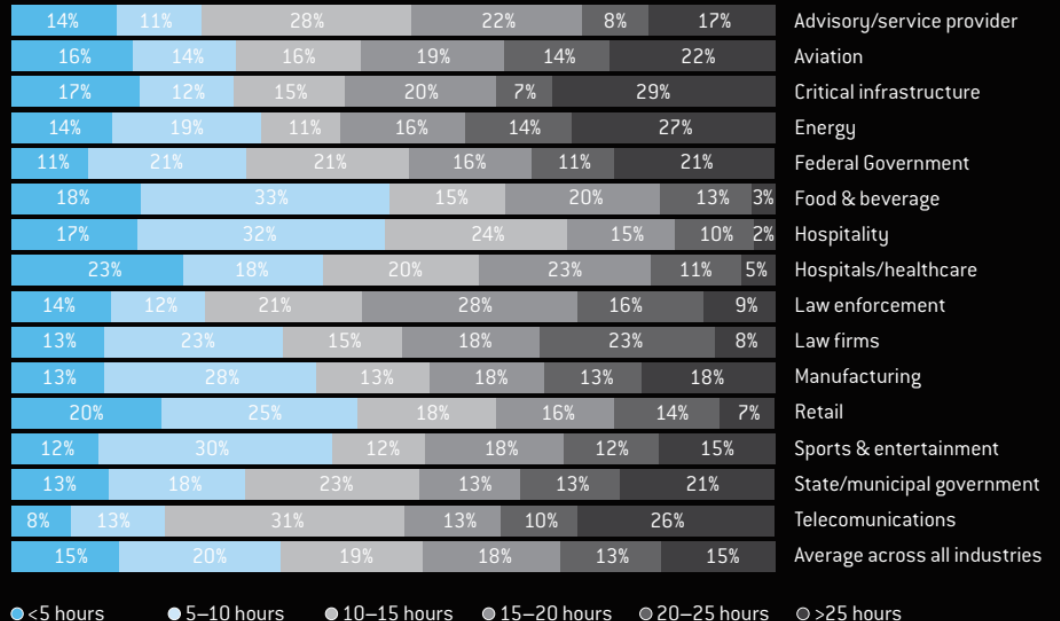
# How to Prevent

## Think Like a Hacker

### THE BLACK REPORT 2018

DECODING THE MINDS OF HACKERS

#### 2. HOW LONG DOES IT TAKE TO BREACH THE PERIMETER, IDENTIFY CRITICAL VALUE DATA, AND EXFILTRATE THAT DATA (COMBINED)?





# How to Prevent

## Think Like a Hacker

6. What is your favorite type of social engineering attack?



**16%**  
Phone



**22%**  
Physical



**62%**  
Phishing

# How to Prevent

What Can You Do?

**1** Use Multi-Factor Authentication



# How to Prevent

What Can You Do?

2

User Learning



# How to Prevent

What Can You Do?

**3** Have an Incident Response Plan (and test it)



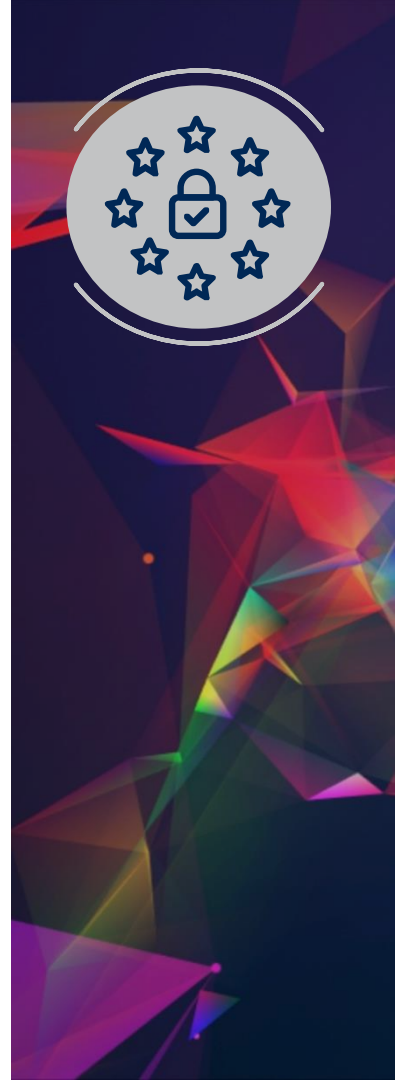


4

# Compliance



# Compliance



# Questions

The background features a large white circle on the left side. The rest of the image is a dark blue gradient with abstract geometric shapes, including colorful polygons and a network of small dots connected by lines, resembling a molecular or data structure.

The image features the Baker McKenzie logo in the top left corner, set against a dark background with a complex, abstract geometric pattern of overlapping triangles in shades of purple, blue, and red. The logo consists of the words "Baker" and "McKenzie." stacked vertically in a white, sans-serif font. The background pattern is dense and multi-colored, with some areas appearing more vibrant than others, creating a sense of depth and movement.

# Baker McKenzie.

[bakermckenzie.com](https://www.bakermckenzie.com)

Baker & McKenzie LLP is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2021 Baker & McKenzie LLP