A Practical Guide to Encryption and Privacy Technologies for Lawyers

Stephen Drew

Dr Fabian Horton

LPLC LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au

Acknowledgement of traditional owners and country

This session is being held on the lands of the Wurundjeri people of the Kulin Nation and on behalf of LPLC I wish to acknowledge them as the traditional owners of the land.

I also acknowledge the traditional owners of the lands which all of those joining us online today are living, learning and working on.

I would also like to pay my respects to their Elders past and present, and any Elders of other communities who may be present today.

Speakers

Stephen Drew

IT consultant and former Microsoft Service Delivery Executive and police forensic analyst. With over 35 years' experience in IT, Stephen has an in-depth knowledge of cybersecurity and encryption technologies.

Dr Fabian Horton

Risk manager with over 20 years of experience spanning both litigious and transactional practice areas. He is a recognised expert in cybersecurity and technology law. He was awarded his PhD in law and technology in 2021.

Today's Agenda

- **What is encryption?**
  Basic encryption technology.
- **Encryption in Microsoft Outlook:**
  Microsoft Outlook encryption tools and IRM.
- **Encryption without IRM:**
  Alternative encryption methods.
- **The role of people in your security model:**
  Why technology alone isn't enough.
- **Q&A**

Poll Time!

How do you feel about sending sensitive information by email?

a) Very concerned

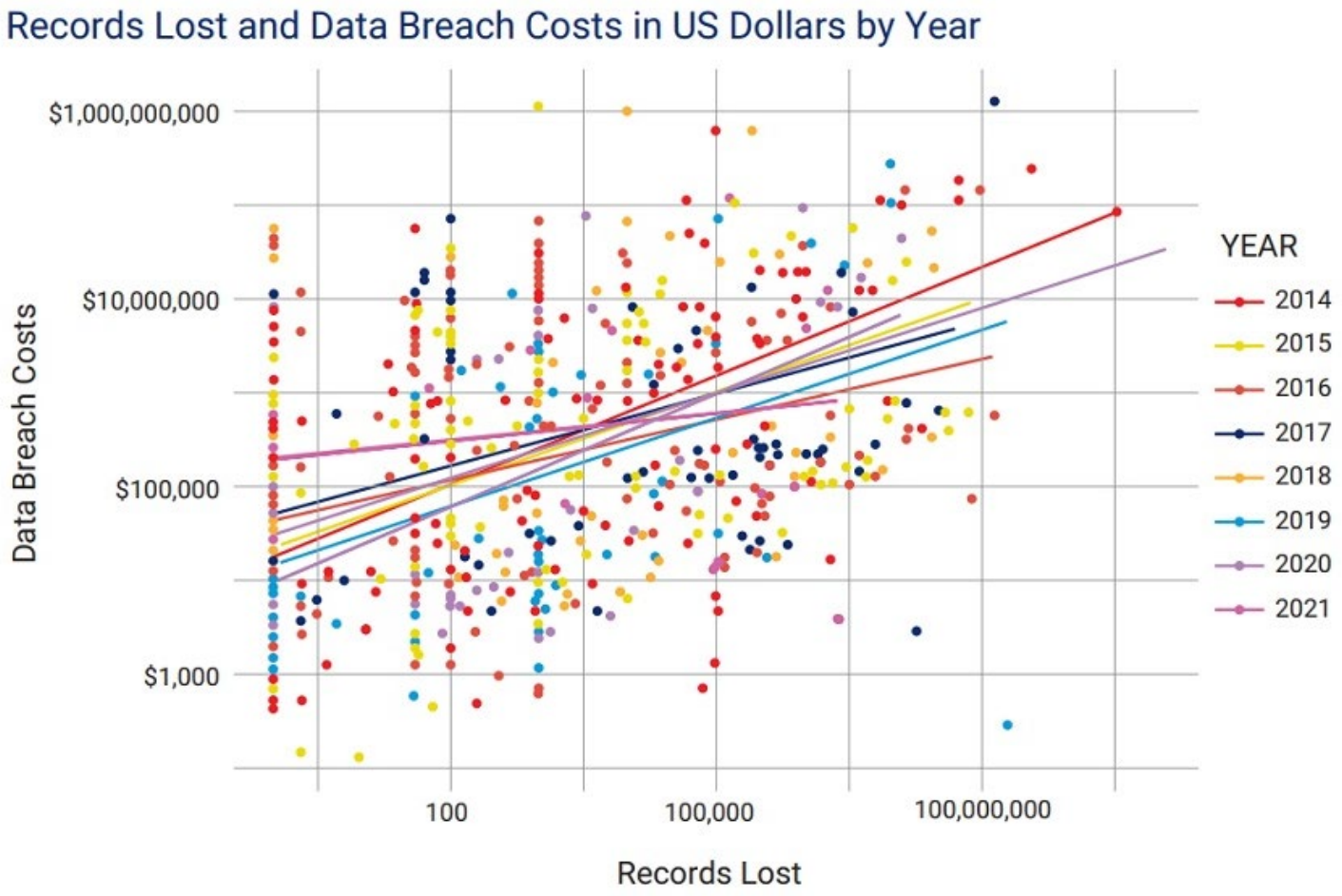
b) A little concerned

c) Not really concerned

d) She'll be right mate

Put your answer in the poll. Responses are anonymous!

The cost of a data breach



The average cost from May 2020 to March 2021 was **US$4.24 million**, or **US$161** per record!

VLSB+C Minimum Cyber Expectations

- Turn on **full disk encryption** for all work devices that store or work with sensitive, confidential or privileged data.
- Ensure all **copies of sensitive, confidential, or privileged data are encrypted** when storing that data (including on external drives and cloud services) and when transferring that data to other organisations.

VLSB+C Minimum Cyber Expectations

- **Only use unencrypted communications** (e.g. email) to send or receive high-risk information (e.g. health information, financial details, identity documents) from clients at their **request and only if strictly necessary**.

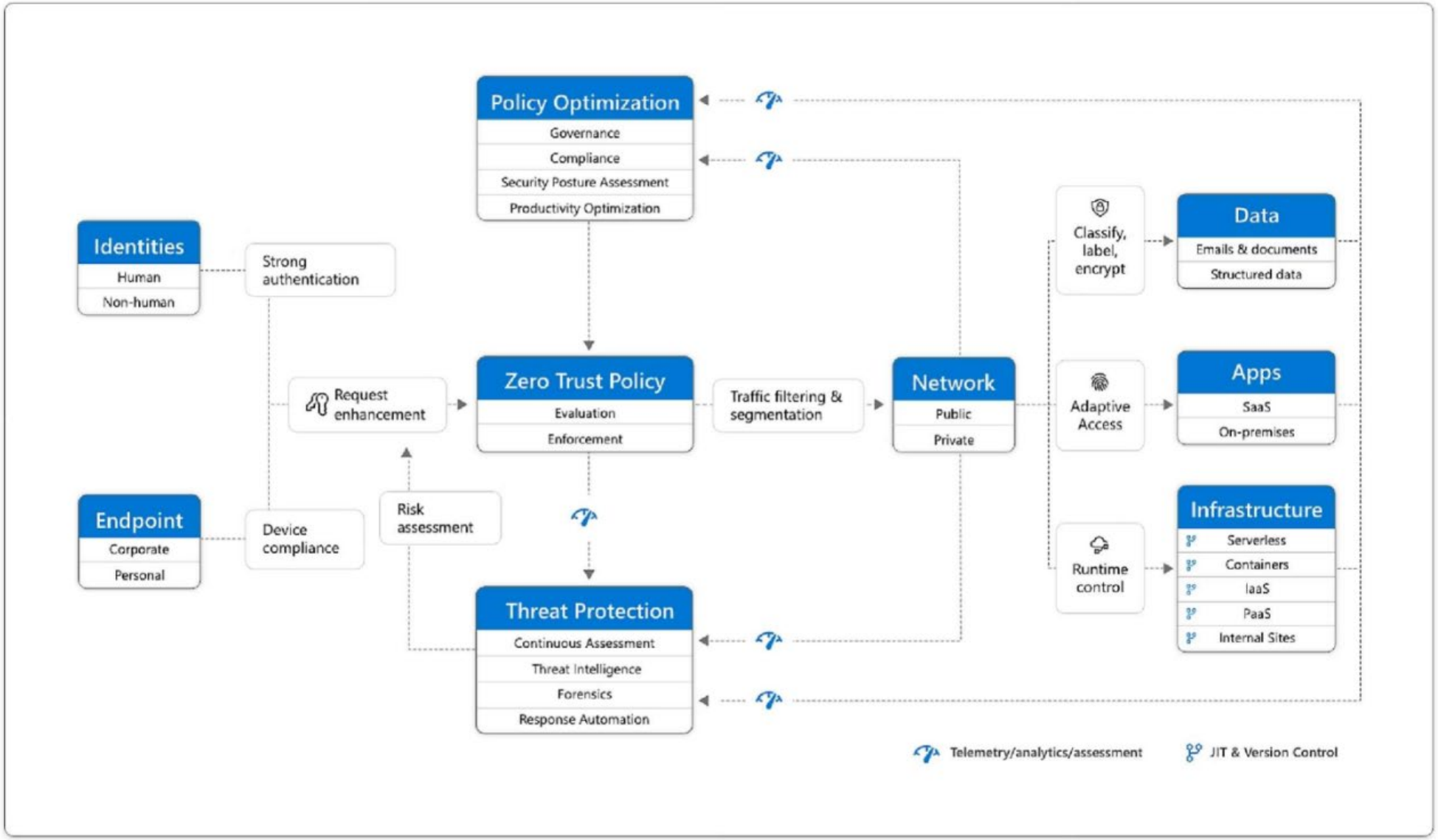
- **Encrypt backups** and store any physical copies in a secure location. Don't store backups in the same location as primary devices, so they are not vulnerable to the same physical incident (e.g. a fire). Ensure recent backups can be accessed quickly.

Non-Encrypted Communications

- A **non-encrypted** connection is when the information being transmitted is in a **human readable format** (e.g. plain text).
- Unencrypted emails have **low security**, making them **easily intercepted** and read by unauthorised individuals.

Microsoft Encryption

Encryption 101: The BIG picture

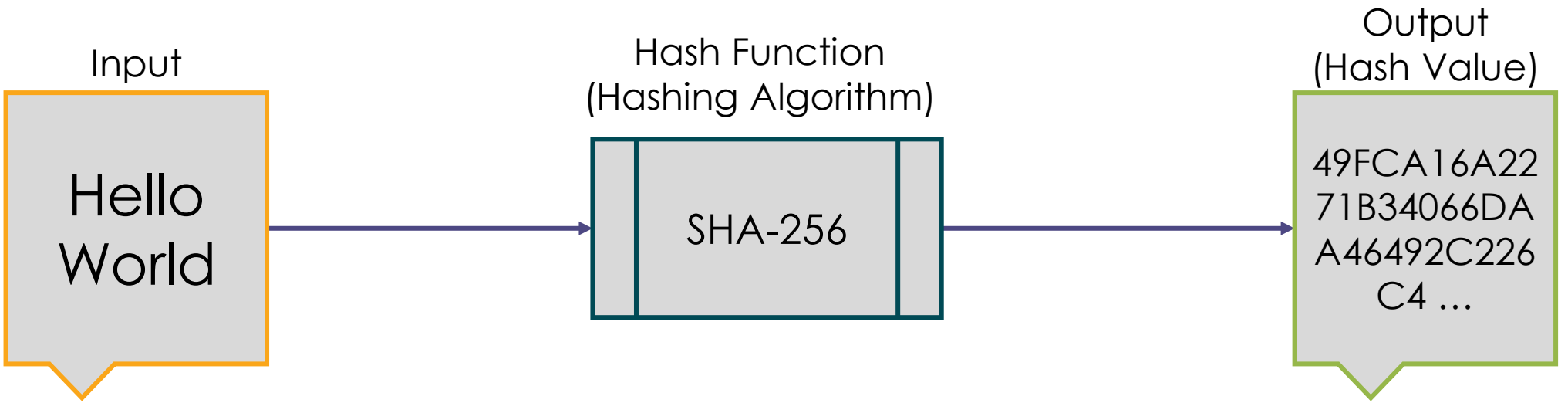


Encryption 101: Why Encryption?

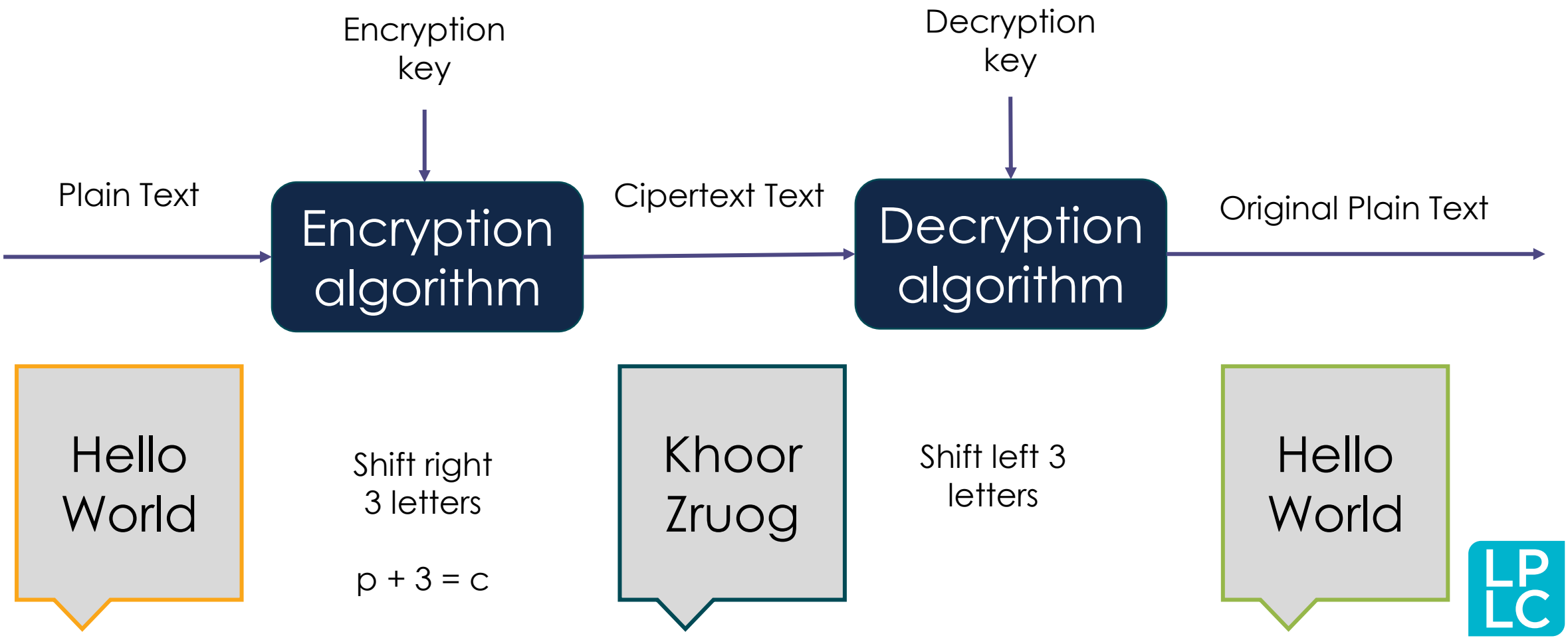
- **Confidentiality (Privacy):**
  Ensure only the intended receiver can read the message.
- **Integrity:**
  Ensure the message has not been altered.
- **Authentication / Non-repudiation:**
  Ensure the sender is who they say they are and that they sent what they say they did.

Encryption 101: Types of Encryption

- **Symmetric Key Encryption:** Single key for both encryption / decryption. Fast but not as strong.
- **Asymmetric Key Encryption:** Public key (encrypt) and Private key (decrypt). Slower but stronger.
- **Hashing**: Converting data into a fixed-length string (hash values).



Encryption 101: Algorithms and Keys



Encryption 101: The 7 Layers of Network Architecture

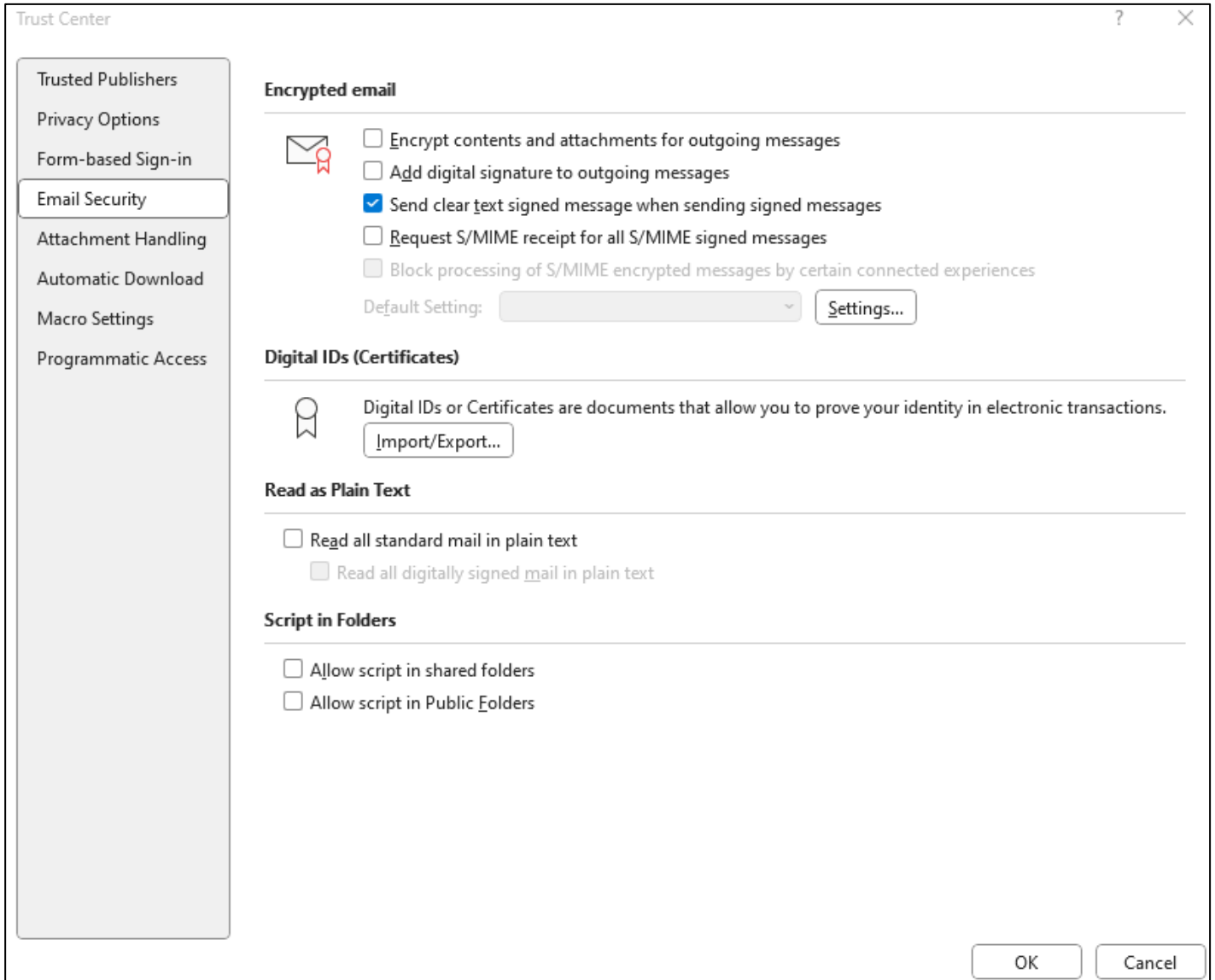
7. Application	• Human-computer interactions • Some encryption
6. Presentation	• Ensure data is in a usable format • Most encryption
5. Session	• Maintains connections and controls sessions • Some encryption
4. Transport	• End-to-end connection and reliability • Some encryption
3. Network	• Decide physical path the data will take • Some encryption
2. Data Link	• Defines the format of the data on the network
1. Physical	• Transmits raw bit streams over physical medium

Encryption in Microsoft Outlook

Microsoft Encryption: What is Used?

Kind of Content	Encryption Technology
Files on a device Computer, tablet, phone or cloud Emails, messages, documents	Device or cloud: BitLocker Data centres: Distributed Key Manager Microsoft 365: Customer Key
Files in transit between users Microsoft 365 documents SharePoint list items between users	Transport Layer Security (TLS)
Email in transit between recipients This includes email hosted by Exchange online	TLS for email in transit S/MIME for email in transit Microsoft Purview Encryption with Azure Advance Protection
Chats, messages and files between recipients using Microsoft Teams	TLS and MTLS to encrypt instant messages Media traffic is encrypted using Secure RTP (SRPT). Teams uses FIPS compliant algorithms for encryption key exchanges

Microsoft Encryption: default settings?



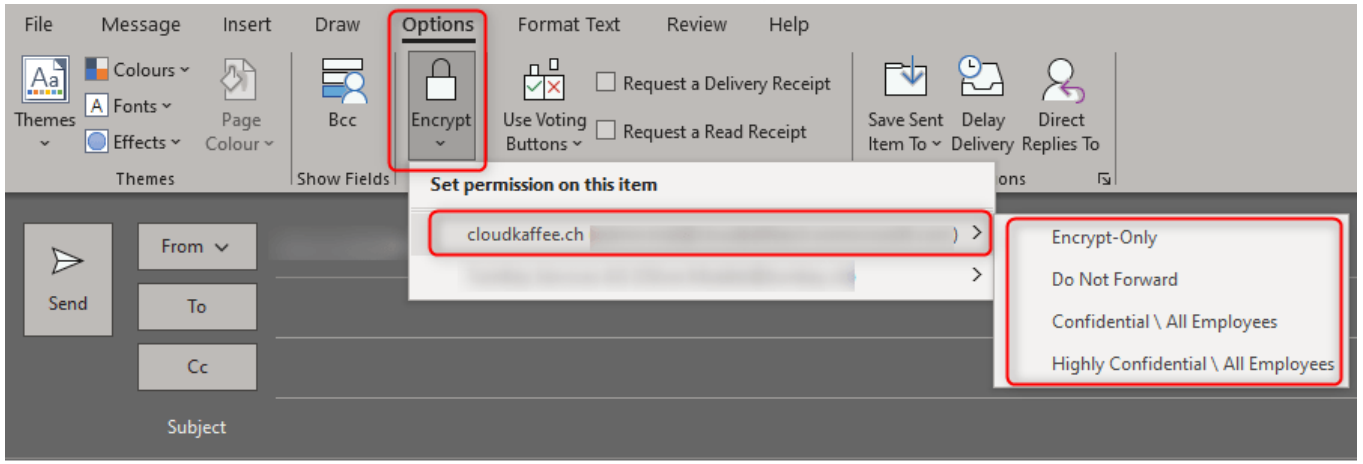
Microsoft Outlook IRM: The Practical

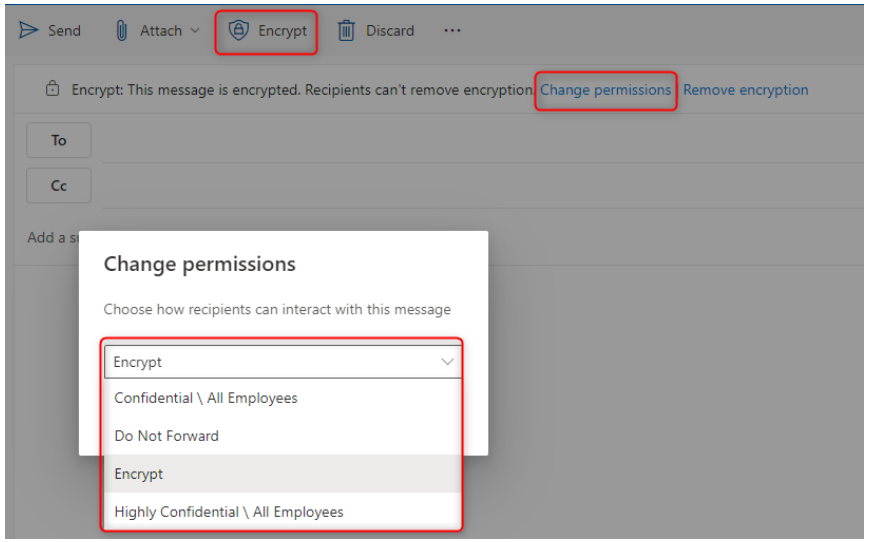
Encrypt-only
Encrypted and recipient must authenticate.

Do not forward
Encrypted and recipient must authenticate.
+ Recipients cannot forward, print or copy email.

Confidential \ All Employees
Encrypted and recipient must authenticate.
+ Recipients can only read, reply to or forward email within the organisation.

High Confidential \ All Employees
Encrypted and recipient must authenticate.
+ Recipients cannot forward, print or copy email.
+ Email can only be read within the organisation.





How IRM Works?

- **Identity-Based Policies**: Controls access by defining who can access the content and what they can do with it. Permissions stored within the content, so it travels with the content.
- **Encryption**: IRM encrypts the content. Only readable with appropriate permissions.
- **Persistent Protection**: The protection policies remain with the content, even outside the organisation.
- **Authentication**: IRM server authenticates reader's identity and checks their permissions.
- **Integration with Microsoft Products**: IRM is integrated with various Microsoft products.

Microsoft Outlook: The Lowdown

- **Is the data on my Windows (Apple) computer encrypted?**
  If enabled.
- **Is the data on Microsoft 365 (including SharePoint) encrypted?**
  Yes.
- **Are my emails encrypted?**
  If enabled.
- **Are my Teams messages encrypted?**
  Yes.

Encryption without IRM

(Application encryption)

Other Encryption: Password Protection for PDFs

You can encrypt your PDF files by applying password protection.

Only individuals with the password can open the document.

Steps:

- Open your PDF in a PDF editor (like Adobe Acrobat).
- Go to the "Protect" or "Security" settings.
- Select "Encrypt" and set a password.
- Save the document.

Tip: Share password with recipient via different method than that used to send the encrypted document (e.g. SMS).

Other Encryption: 3rd Party Encryption Tools

There are third-party tools available that can encrypt your emails and attachments. These tools often use **strong encryption algorithms**.

Popular Tools:

- **GPG** (GNU Privacy Guard): A free implementation of the OpenPGP standard that allows you to encrypt and sign your emails and files.
- **VeraCrypt**: Can encrypt files and create secure containers for sensitive information.
- **AxCrypt**: A user-friendly file encryption software that integrates with Windows.
- **Encrypted email programs:** There are numerous secure email providers.

Other Encryption: 3rd Party Portals

There are secure portals that are effective for sending confidential documents.

There are many product offerings including some that are available through popular practice management systems.

Features to consider:

- **Robust Security Measures:** End-to-End Encryption, Multi-Factor Authentication (MFA) and Regular Security Audits.
- **Document Management Features**: Audit Trails, Version Control, eSignatures.
- **Notifications and Alerts**: Real-Time Notifications and in-app messaging.
- **Customisation:** White-labelling and custom permissions.
- **Analytics and Reporting**: Including activity tracking.

People, Systems, Processes

Tips for keeping your data safe

- Make sure your people are trained.
  9 in 10 data breach incidents are caused by employee mistakes.
- Create a strong account password and use two-factor authentication.
- Share but in a protected way.
- Put extra sensitive information in a vault.
- Choose the most secure cloud provider.

Personal Vault

Personal Vault automatically locks after a period of inactivity and then you need to unlock it to get to your files again.

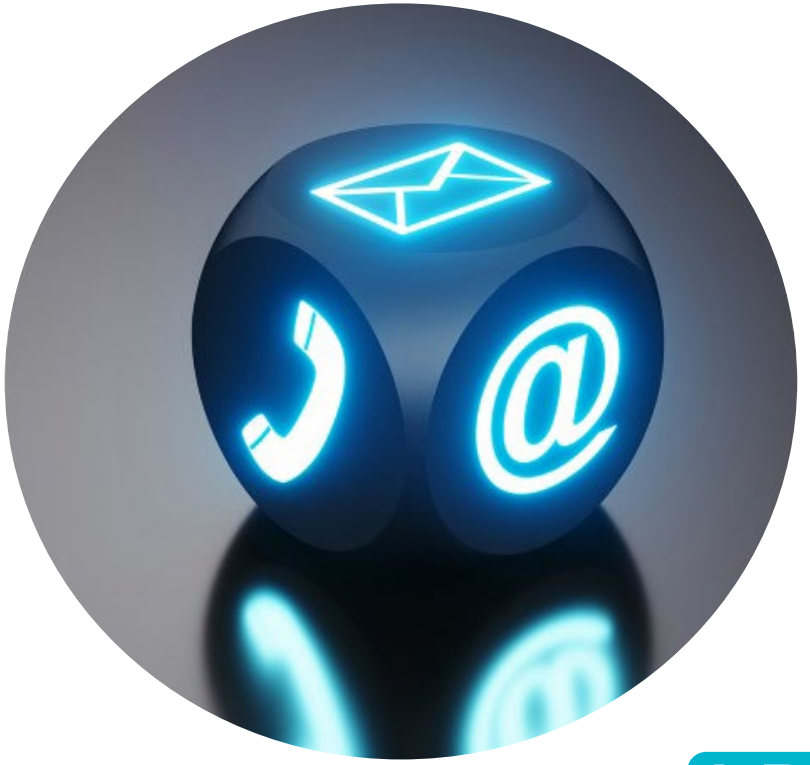
FUN FACT: Did you know that by simply choosing a 12-character password (pass-phrase) over a 6-character password, it would take 62-trillion times longer for a computer to hack it?

Q&A

Get the latest LPLC news and alerts

Subscribe to the latest risk management updates, events, news and alerts by visiting:

lplc.com.au/subscribe



Thank you

LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au