CrucialLogics
consulting with a conscience

Packetlabs

# CLOUDY with a chance of DATA LEAKAGE

# Thank you for joining us today!

- This session is being recorded for replay
- Listen-only mode during the presentation
- Ask questions!  Please submit questions via the chat

# Speaker

## Amol Joshi

**Partner Enterprise Services, CrucialLogics**

Amol is a senior security executive with over 16 years of experience in leading and executing complex IT transformations and security programs. He's a firm believer in achieving security through standardization, avoiding complexity and that security be achieved using native, easy-to-use technologies. Amol approaches business challenges in a detail-oriented way and demonstrates quantifiable results throughout the course of highly technical and complex engagements.

# Speaker

## Richard Rogerson

**Managing Partner, Packetlabs**

Richard leads a team of ethical hackers who find critical vulnerabilities in client systems before a breach. He has 10+ years of professional consulting experience delivering and leading offensive campaigns. He has several of the most advanced cybersecurity certifications and has been featured in the media several times for his views on cybersecurity breaches including Business E-mail Compromise, Ransomware and Nation-state APTs.

# Speaker

## Desirae Huot

**Principal Consultant, Enterprise Services, CrucialLogics**

Desirae has 15+ years of experience in information architecture design and governance, designing corporate intranets, cloud migration, system integration, data analytics, process automation, and business transformation to the modern workplace. She enjoys working collaboratively with clients to maximize employee experience by leveraging modern technologies to uncover opportunities for improvement, automation, and evolution of business processes.

# Today's Agenda

- Data leakage
- Example scenarios
- Access control
- Data Loss Prevention
- Sensitive data
- Classification
- Information protection
- Auto labeling

# Data Leakage

**Data leakage** is the unauthorized transmission of data from within an organization to an external destination or recipient. Data leakage can happen accidentally, or it can be a result of the actions of people internally or externally with malicious intent.

**Why should you care about data leakage?**

- Personal, financial and health information can be sold and used for marketing, fraud and identity theft.
- Intellectual property can be sold and used to develop products and services similar to those of your business.
- Competitive information can be sold and used by your competitors to block your strategic plans and leaked legal information may damage your legal position.
- Data on IT security is a valuable target in itself because it lets the unauthorized parties gain access to all the other types of information on your system.
- Protecting this type of data is vital as the impact of it being leaked can easily lead to identity theft, revenue loss, reputational damage, operational disruption, regulatory sanction, and potential lawsuits.

# Threats to Data Leakage

**There are various threats that target sensitive information:**

1. **Ransomware –** If you do not pay the ransom, they threaten to leak your data.
2. **State sponsored APTs –** Vaccine research was targeted during the COVID-19 pandemic.
3. **Hacktivist –** Anonymous vs Russia
4. **Lapsus$ -** International Hacking gang (NVIDIA, Microsoft, Okta, etc.)
5. **Competitors -** Less frequently, we hear about competitors trying to obtain access to trade secrets of their competitors.
6. **Disgruntled Employees –** Insider threats still present a credible risk. We've seen numerous cases of employees being paid to provide access to attackers.

# Know Your Data – Classification

## PUBLIC

**Data that can be freely shared with anyone**

- Marketing material
- Press releases
- Job postings
- Company contact information

## INTERNAL

**Data shared within the organization**

- Employee handbook
- Budgets
- Project plans
- Work schedules

## CONFIDENTIAL

**Data shared with select internal individuals as needed for their jobs**

- Merger/acquisition information
- Employee reviews
- IT security information
- Business strategies

## RESTRICTED

**Data that is highly sensitive**

- Personally identifiable information
- Health information
- Financial information
- Trade secrets

Attackers target

# Attacker Targets / Objectives

## Identity Theft / Fraud

### Personally Identifiable Information

- Social insurance numbers
- Passport numbers
- Driver's license numbers

### Financial Information

- Credit card numbers and expiry dates
- Bank account numbers
- Investment statements

### Health Information

- Personal health identification numbers
- Medical records

## Extortion / Ransom / Espionage

### Intellectual Property

- Product drawings & specifications
- Trade secrets
- Proprietary materials that the business has developed

### Competition Information

- Market studies
- Business relationships
- Pricing information
- Business plans

### Legal Information

- Court cases the company may be pursuing
- Merger and acquisition details
- Regulatory rulings

## Ransomware / Supply-Chain

### IT Security Information

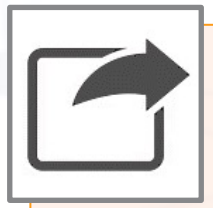
- Usernames
- Encryption keys
- Security strategies
- Network diagrams

# Data Leakage Scenarios

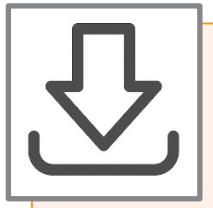
An employee accidentally chooses the wrong recipient when sending an email containing confidential data in the contents of the email or in an attachment.

A guest is invited to the Finance department's Microsoft Team where the organization's budgets and internal financial data is stored.

An employee sends a list of credit card numbers in a Microsoft Teams chat.



A file stored on SharePoint that contains personally identifiable information is shared with someone outside the organization.



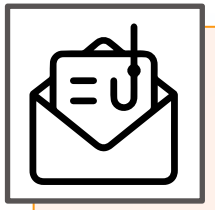
An employee downloads a copy of a document containing a social insurance number and uploads it to their Google Drive.

A manager creates a Power Automate flow that saves email attachments in their personal Dropbox whenever they receive an email in their corporate mailbox.

# Stories From The Red Team

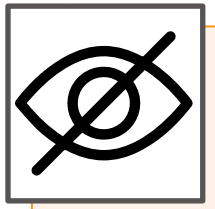
A low privileged user is compromised and their e-mail is searched for credentials/spreadsheets/certificates.


An inactive employee's account is compromised via password spraying and leveraged to obtain access to key departmental shares.

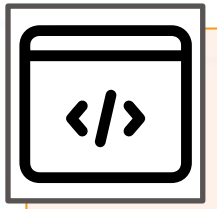


An employee is asked for sensitive information over a compromised Teams account (e.g., password reset, spreadsheets, credentials)

An employees RDP session is hijacked enabling access to corporate ERP solution including customer information and pricing.



A compromised user account is used to search Microsoft SharePoint and File Shares for sensitive content.



A logon script is found that contains Domain Admin credentials that enables the compromise of corporate backups.

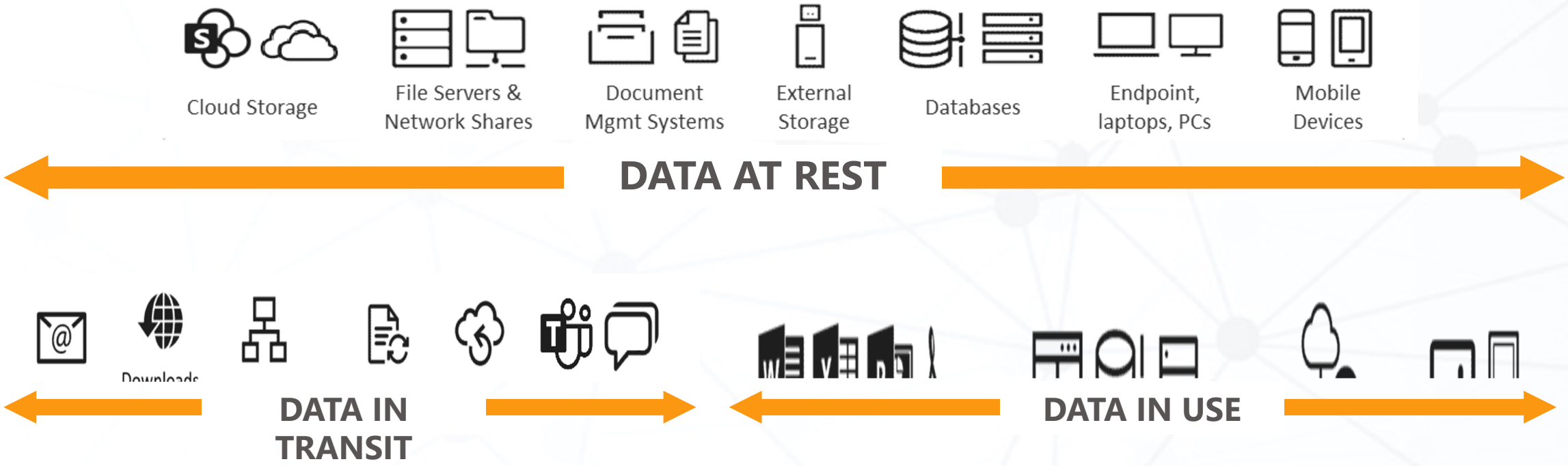
# Information Protection Lifecycle

# Protect Your Data - Access Control

- Use permissions in Teams, SharePoint, and OneDrive to provide or restrict user access to the site and its contents.
- Disable external sharing and anonymous links when not needed and restrict sharing to specified domains.
- Set up conditional access policies to enforce MFA and web-only access for guests, and disable their ability to download, print, or sync files to their device.
- Automatically sign out users who have idle browser sessions
- Automate periodic access reviews to ensure users do not retain access to your organization's sensitive information for longer than is necessary.
- Create Power Platform environments to manage access and apply DLP policies to control which types of connectors can be used to prevent users from exposing data outside of the organization.

# Sensitivity Labels

Protect data inside and outside your organization no matter where it resides



# Prevent Data Loss – DLP Policies

Data Loss Prevention (DLP) policies helps organizations prevent the unintentional or accidental sharing of sensitive information. You can identify, monitor, and automatically protect sensitive content across several services.

# Data Retention

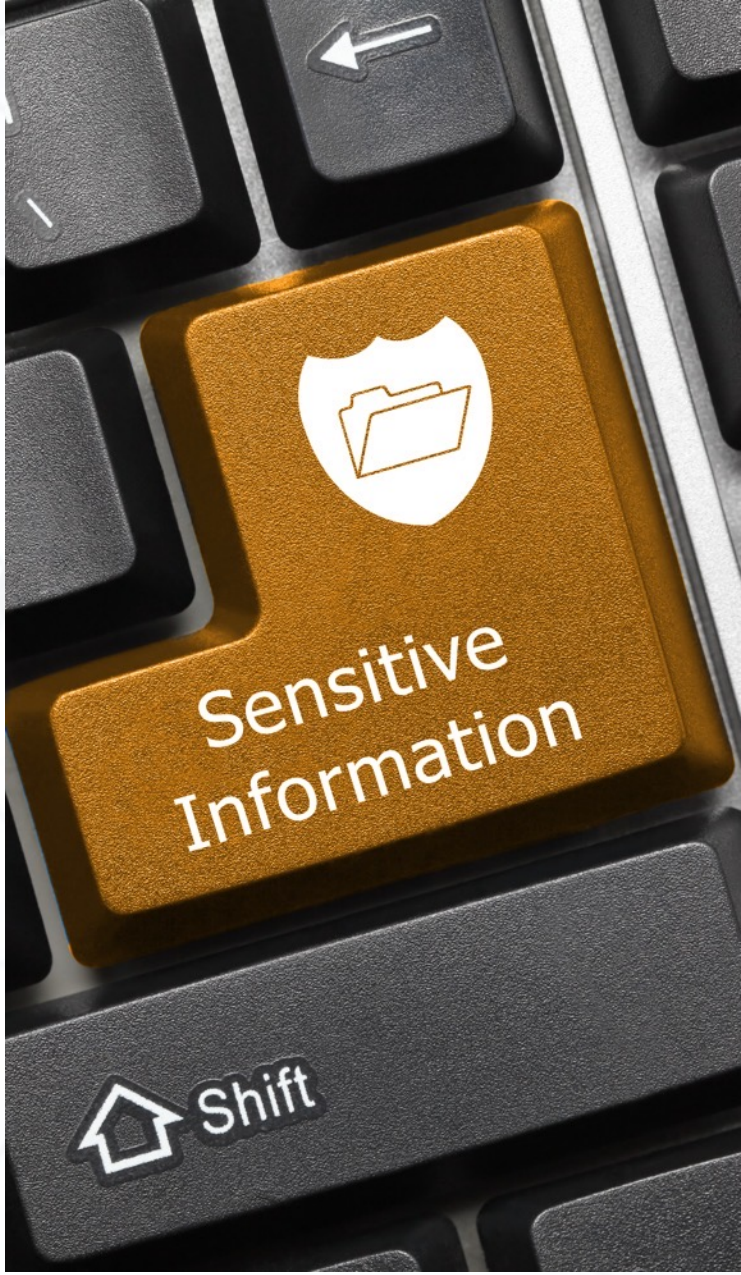
Retention policies establish rules for storing and destroying information to comply with regulatory compliance requirements.

**Risks of retaining information indefinitely**

- Sensitive information such as social insurance numbers and birth dates are not content that gets outdated so retaining that information unnecessarily increases the risk of it being leaked.
- If you were to suffer a data breach and regulators were to find that data had not been destroyed as required, not only could you be fined, but you could also lose the trust of your customers and employees.

**Benefits of implementing a data destruction policy**

- Data protection laws worldwide such as GDPR, SOX, and HIPAA state clear rules for consumers' right for their information to be erased and forgotten. Data destruction policies ensure that these guidelines are met.
- Information is only retained when it is in use and for as long as necessary before it is safely disposed of and is no longer a risk.



# Govern Your Data – Auto Labeling

Sensitivity labels and retention labels can be automatically applied based on sensitive information that is detected in the content or based on how the content has been classified.

**Benefits of auto labeling content**

- You don't need to train your users when to use each of your classifications.
- You don't need to rely on users to classify all content correctly.
- Users no longer need to know about your governance policies—they can instead focus on their work.

**Manage compliance at scale**

***Trainable Classifiers*** use machine learning to identify the type of content and automatically apply a sensitivity label and retention label.

***SharePoint Syntex*** is an add-on that uses advanced AI and machine learning to automate content processing. It can be used to identify the type of content, extract metadata from within the content, and automatically apply sensitivity and retention labels.

# Verify Data is Protected

After controls have been applied to your data, consider a Red Team or objective-based Pentest to validate whether or not the controls are effective.

**Risks of Implementing Controls Without Testing**

- False sense of security if assumptions are not validated (attackers can't get to that share).
- Potential exposure of sensitive information on less-secure environments (development, e-mail, unencrypted laptops).

**Benefits of Red Team or Objective-Based Pentest**

- Understanding whether controls are effective
- Validation that the Incident Response Plan is complete ("Cyber fire drill")
- Continuous monitoring and improvement based on attacker techniques

# Questions For You

- What is your high-value and high-risk data and do you know everywhere it has been saved?
- How often do you review group membership and permissions both internally and for guest users?
- What compliance requirements does your organization need to adhere to?
- What will be your biggest challenge in rolling out a proper information protection strategy?

# Questions?

**To ask our speakers a question,** type your question into the Chat located in the bottom right portion of the screen.

# What's Next?

Take advantage of our experts to book an assessment, at no cost to you.

**How To Get Started**

- Respond to our webinar follow up email to book your assessment before May 31
- Download the additional information and resources in our follow up email

# Thank you for joining us today.

**Amol Joshi**
CrucialLogics
Amol.Joshi@cruciallogics.com

**Richard Rogerson**
Packetlabs
Rogerson@packetlabs.net

**Desirae Huot**
CrucialLogics
Desirae.Huot@cruciallogics.com