Strategies to Safeguard Sensitive Information

Rose Lally - CISO and VP, Governance & Controls at Altisource

October 17, 2024

Agenda

- Brief intro
- Personal data protection
- Assess your risk posture first
- Strategies for Safeguarding Sensitive Information
- Wrap Up and Questions

Brief Intro – Rose Lally

Rose began her career as a software engineer in customer support and implementations for healthcare information systems then went on to leadership positions in eCommerce, data center hosting, operations, business continuity and disaster recovery. She then led a Technology Services organization, responsible for the service desk, infrastructure, vendor management and information security at a global manufacturing company. Upon joining Altisource in 2014 she built the technology Governance & Controls program, began leading information security in 2018, vendor management and facilities management since 2020. Rose received her MBA from Bentley University and lives near Boston with her family

Personal Data Protection

What personal data do you want protected?

social security, and other government issued numbers

geo location data

address book

Medical records

logins & passwords for online accounts

credit card numbers

Email addresses

photos & videos

vehicle registration number

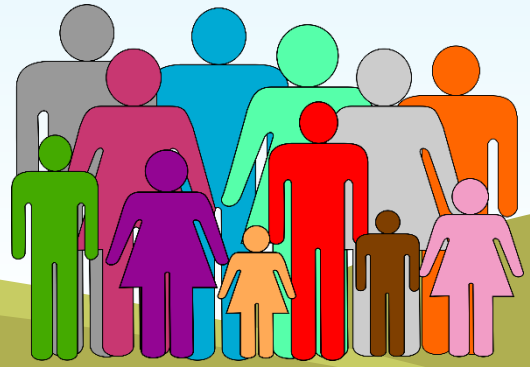
Date of birth

home address

passport information

financial credentials

Mother's maiden name



*Data Source: https://usa.kaspersky.com/internet-security-center/infographics/identity-theft-personal-data-infographic#.WJGC71N950w

What's happening out in the world of data breaches

Company / Organization	Year	Impacted Users
MGM Grand	2020	10 million
LinkedIn	2021	700 million
T-Mobile	2023	37 million
23andMe	2023	20 million
National Public Data	2024	Millions of social security numbers, Billions including the deceased
AT&T	2024	7.6 million current customers, 65.4 million former customers
Ticketmaster	2024	560 million
Dell	2024	49 million

Data security risk statistics

64% of Americans have never checked to see if they were affected by a data breach

94% of malware is delivered via email

44% of users report recycling passwords across personal and business related accounts

~60% of data leaks occur due to exploited, unpatched vulnerabilities

In 2022, the Federal Trade Commission received more than 1.1 million reports of identity theft

95% of cybersecurity incidents are ***due to human error***

Over 75% of targeted cyberattacks start with an email in 2024, making phishing a primary vector for cybercrime

78% of people claim to know the risks that come with clicking unknown links in emails and ***yet still click these links***

Source: https://www.varonis.com/blog/cybersecurity-statistics/

What bad things can happen with stolen personal data?

- **SCAM YOUR CONTACTS**
- **HACK YOUR DEVICE**
- **STEAL YOUR IDENTITY AND MONEY**
- **BURGLARY**
- **INSURANCE & BANK LOAN FRAUD**

Assess your risk posture

Assess your personal risk posture

What is risk?

The potential for uncontrolled exposure to danger, harm or loss

What is your risk tolerance level?

Think about your home security

- What are you protecting yourself from?
- Are you trying to protect anything inside the house from getting out?
- What is the likelihood of these different risks occurring?
- What is your appetite for risk?
- What are your known vulnerabilities?
- What compensating controls have you put in place to get to a tolerable level of risk?

Assess your company's risk posture

What are your hard guard rail requirements?

- Audits, regulations, contractual obligations, other?

How aware/educated are employees on data security?

Do you know your vulnerabilities?

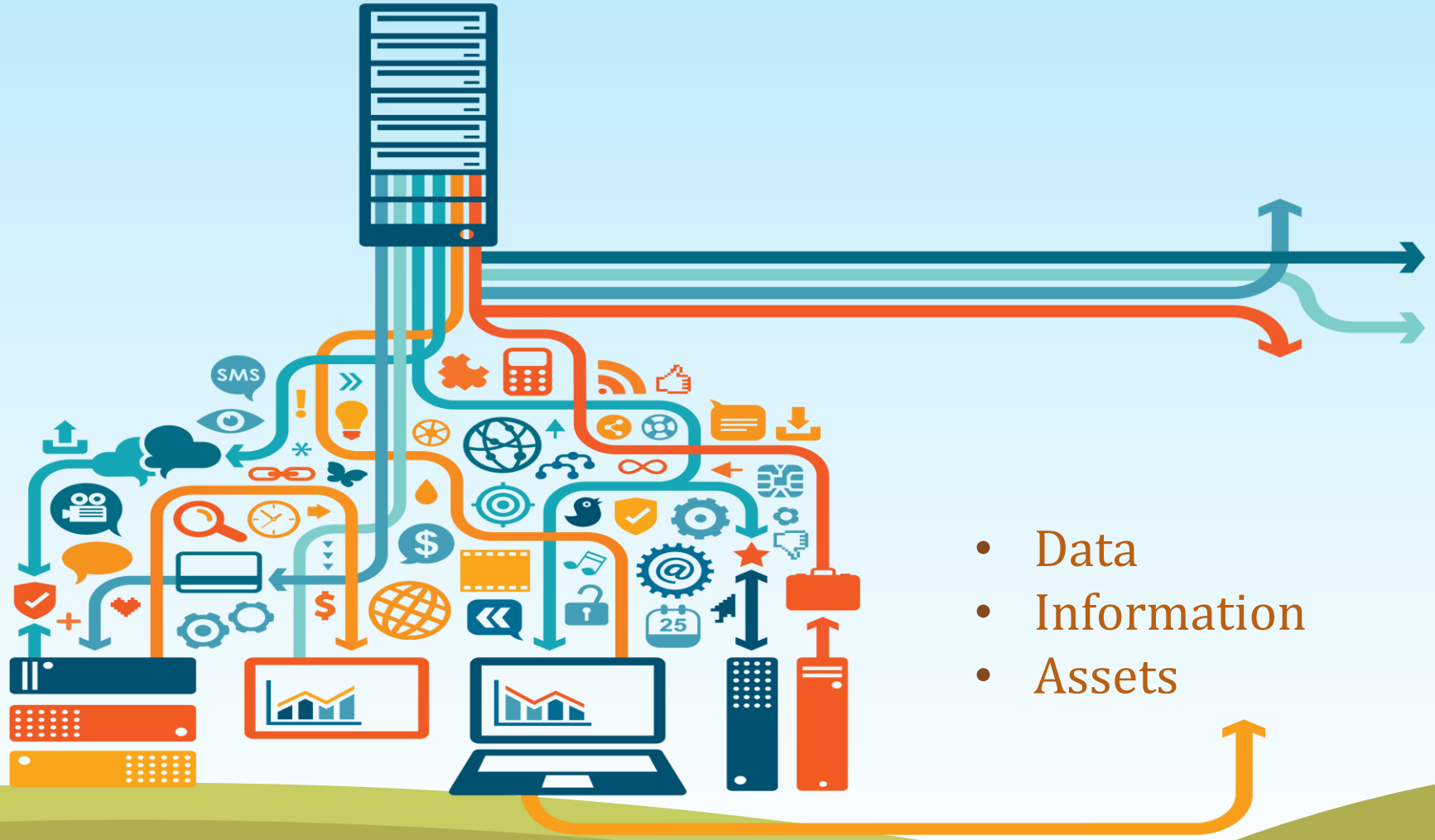
Estimate the potential damage if your company is hit with a major data breach, phishing incident or ransomware attack

How aligned is your security budget, including resources?

What level of risk is your company willing to tolerate?

Strategies for Safeguarding Sensitive Information

What are you safeguarding?



- Data
- Information
- Assets

Safeguarding sensitive information

Information is a set of data that is meaningful to a person or an organization

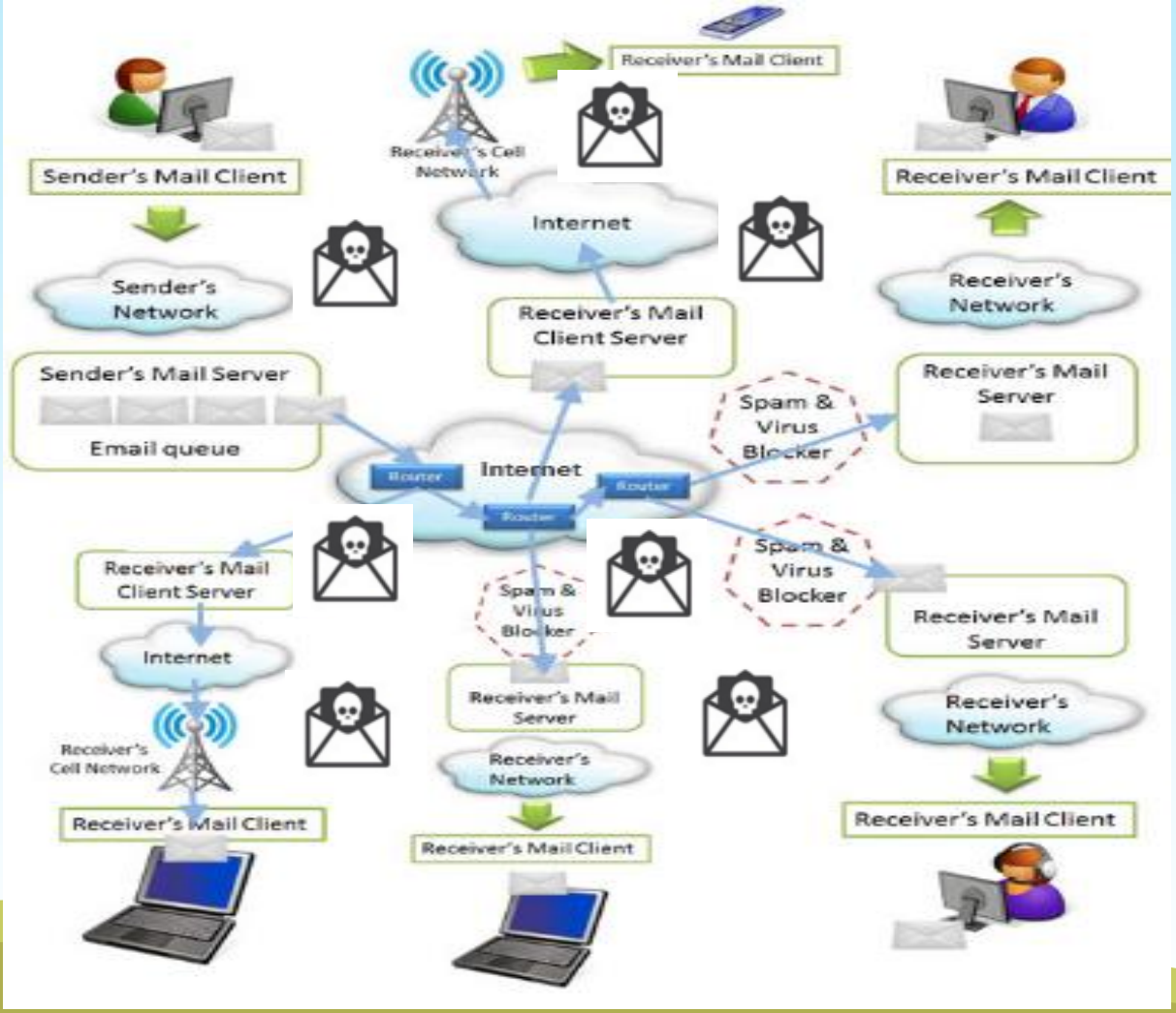
Information considered sensitive by you, your company, regulations, or consumers needs to be handled properly in transit and at rest

An Information Asset is any asset used for storing, processing, transmitting or disposing information

Where information may reside or travel:

- Stored on desktops, laptops, servers, phones, printers
- Emails – internal and external
- Paper – printed or written
- Online videos
- Public WiFi
- Company network
- 3rd party vendors

How Emails Travel – Riskier And More Complex Than It May Seem



Think about how many emails do you send and receive in a day

How many recipients are on those emails?

How many times do they go back and forth?

Information security risk increases with the # of recipients involved, the number of times the email goes back and forth, lack of encryption of sensitive information, and use of personal email addresses

*Data Source: http://help.theatremanager.com/frequently-asked-questions/how-e-blasts-work

*general depiction, does not represent any company's actual email system

Information Security Maturity Model

Level 0 – Blissfully Unprepared

- No policies or standards
- No information security tools
- Lacking necessary information to take effective action
- Unaware or unable to respond to issues
- Stakeholders oblivious – no employee education on security

Level 1 – Reactive, starting to reduce risk

- Established Information Security Policies & Standards
- Have basic tools and structures to react to to business requirements
- Cannot proactively prevent problems from arising
- Vulnerability backlog
- Educating employees
- Stakeholder reluctance

Level 2 – Defined, compliance focused

- Data is encrypted in transit and at rest
- Data Loss Prevention tools in place
- Established controls for Policies & Standards
- Role based, least privilege access
- Have tools, structure, processes to proactively address current issues and challenges
- Managing vulnerabilities effectively
- Employees educated
- Stakeholder buy-in

Level 3 – Risk based, Anticipatory

- Have tools, structure, organizational processes to proactively address future issues and challenges
- AI & Automation
- Hunt threats
- Behavior trending
- Understand current and future risks tied to business strategy
- Risk based decisions
- Stakeholders autonomous and proactive

Level 4 – Continuous Improvement

- Optimal security program
- All security risk areas continuously monitored, initial responses to security incidents automated
- All information classified and labeled

Strategizing - It's all about risk

1. Determine what risk areas are applicable to your company and assess risk posture
2. Get internal agreement on your current cybersecurity maturity level and what level of maturity the company wants to strive for
3. Prioritize compensating controls implementation
4. Roadmap the game plan by year at a reasonable pace, considering budget and resource constraints

2024	2025	2026	202?
Level 0 **Blissfully unaware**	**Level 1** **Reactive, starting to reduce risks**	**Level 2** **Defined, compliance focused**	**Level 3** **Risk based & anticipatory**	**Level 4** **Aligned with business and continuously improving**

Wrap Up and Questions

Ensure you have reasonable situational risk awareness

Understand what your security requirements are

Right-size your cybersecurity protection at work and at home