

# Cybersecurity Workshop: What Every Art Organization Needs To Know



With Annika Erikson,  
Founder & CEO of Articheck





# Today:

## CYBERSECURITY WORKSHOP

- Art world cybersecurity concerns
- Important insurance industry news
- Actions to take right now to protect your data

# ART WORLD CONSEQUENCES

- THEFT
  - location
  - value
- Reputation damage
  - client data
  - artist data
- Monetary loss
  - institution funds
  - client money
- Fraud
  - taking
  - adding info
- Loss of control
  - can't work!



# WHY HACKERS TARGET THE ART WORLD

75% of cyber attacks target companies with 11-1,000 employees. They are often an easy target with less robust cyber security controls (or none at all). Art galleries are a particularly tempting target with:

- High-value items
- Connections with HNW individuals (whose contacts, networks and bank accounts can be further compromised)

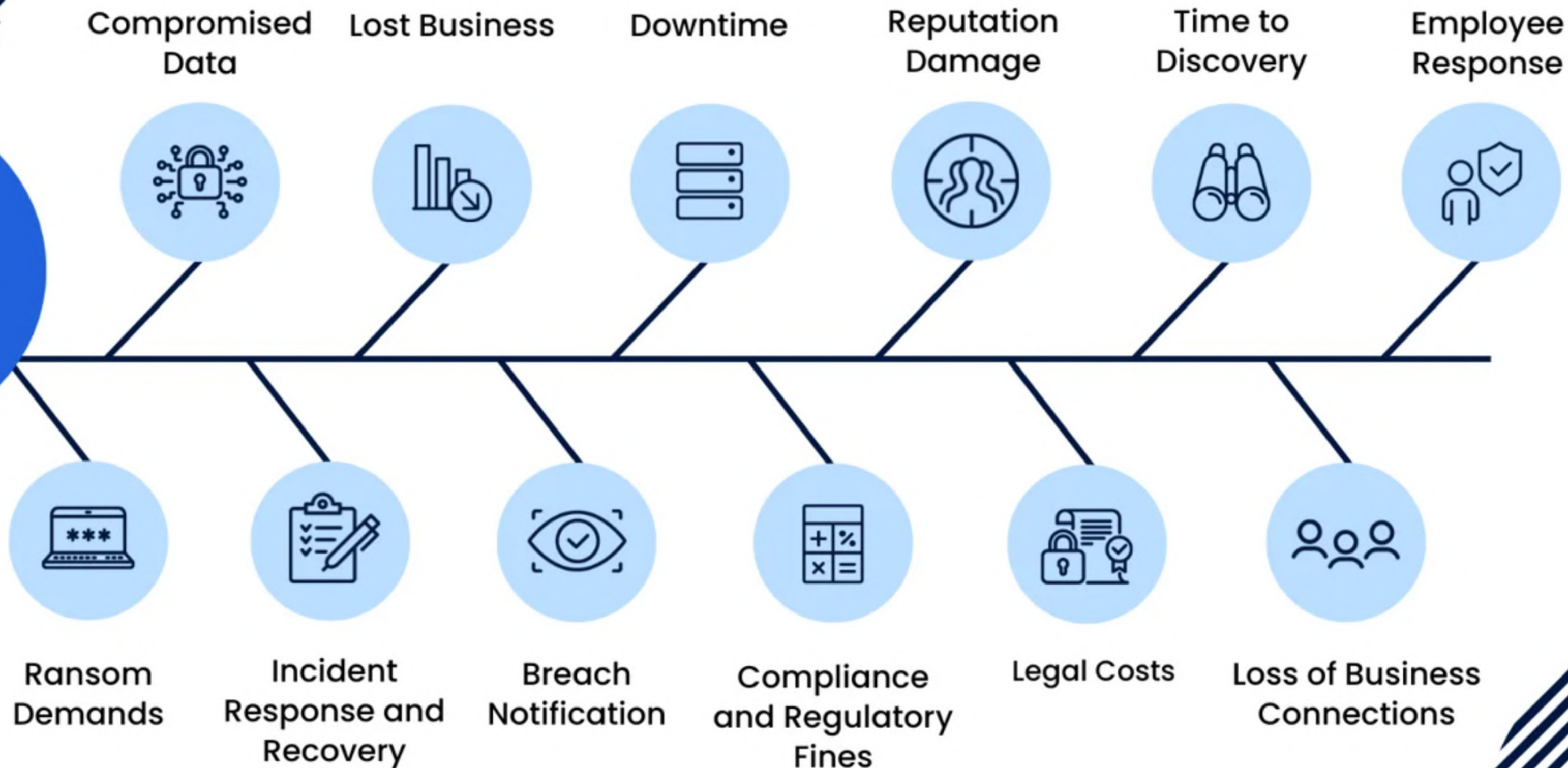
# WHY HACKERS TARGET THE ART WORLD

Art organisations are a particularly tempting target (cont.):

- Technology dependant:
  - Data collection – collectors, members, patrons, visitors and employee
  - Partners and suppliers may have access to organisation network
  - Staff vulnerability – accidental or rogue employee

# The True Costs of a Security Breach

**12 COSTS FROM A SECURITY BREACH**



artnet news

Crime

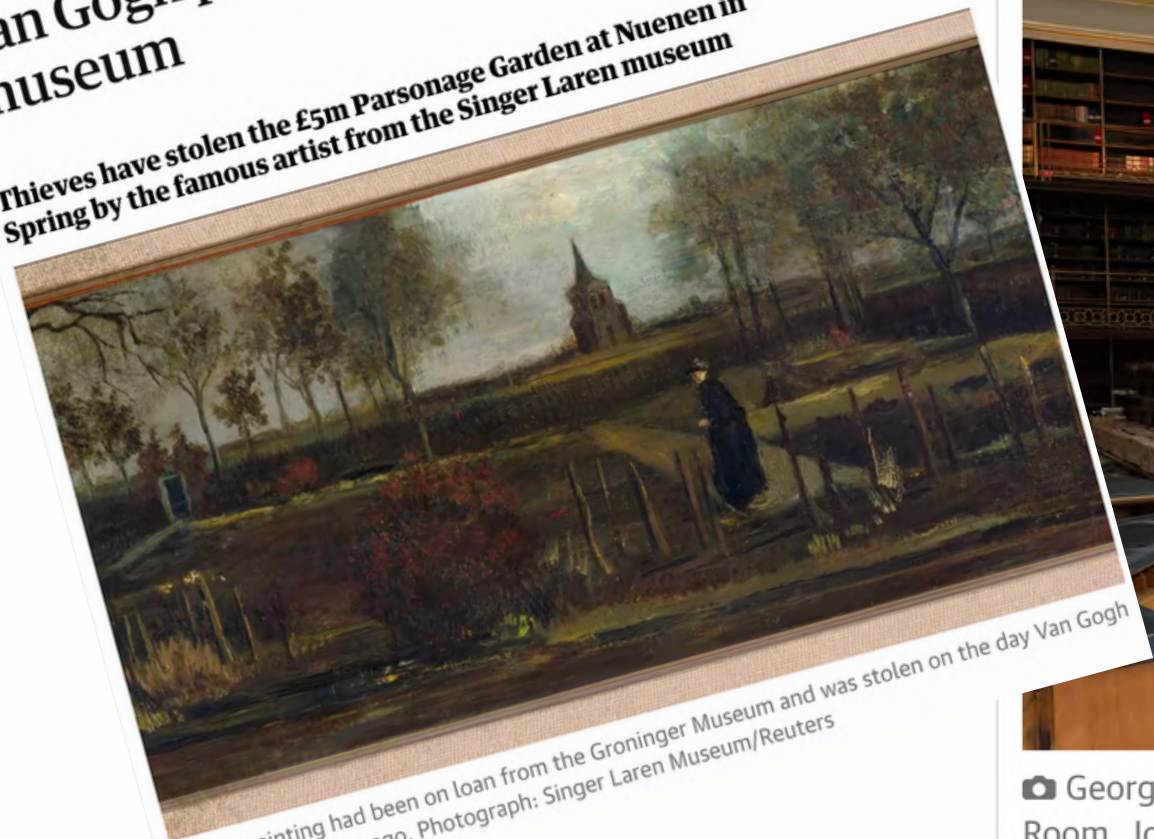
### A German Museum Employee Has Been Caught 'Shamelessly' Swapping Original Paintings for Fakes to Fund His Lavish Lifestyle

The man is said to have spent the money on a new apartment and a Rolls-Royce.

Jo Lawson-Tancred, September 25, 2023

### Van Gogh painting stolen from Dutch museum

Thieves have stolen the £5m Parsonage Garden at Nuenen in Spring by the famous artist from the Singer Laren museum



The painting had been on loan from the Groninger Museum and was stolen on the day Van Gogh was born 167 years ago. Photograph: Singer Laren Museum/Reuters

The New York Times

### Auctioneer Admits to Helping Create Fake Works Shown as Basquiats in Orlando

The man has agreed to plead guilty to a charge of lying to federal agents who say he had displayed and later seized...



The Guardian

## British Museum thefts were 'inside job', says George Osborne

Chair of trustees tells MPs security has been tightened and that recovered items will go on display



George Osborne (left) and Mark Jones, the interim director, in the British Museum's Reading Room. Jones said the museum wanted to increase access to its collections. Photograph: Aaron Chown/PA

The New York Times

### British Museum Announces Plan to Stop Thefts

The museum will overhaul its record keeping, but its leaders said that millions of items still would not be individually documented.



Five men convicted of audacious Dresden jewel heist

16 May



British Museum thefts: What we know so far

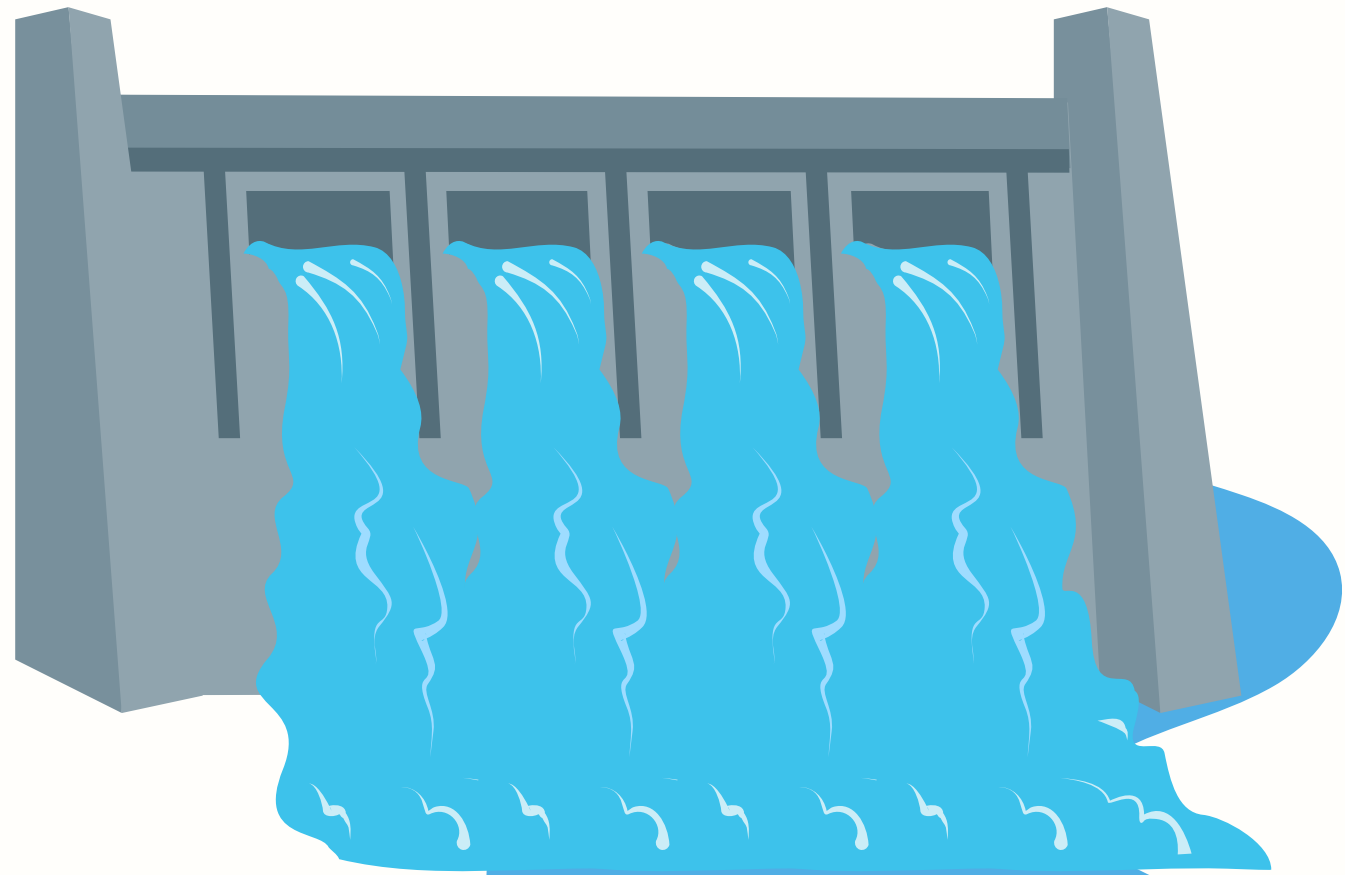
26 August

Historic objects stolen from Kelham Island Museum



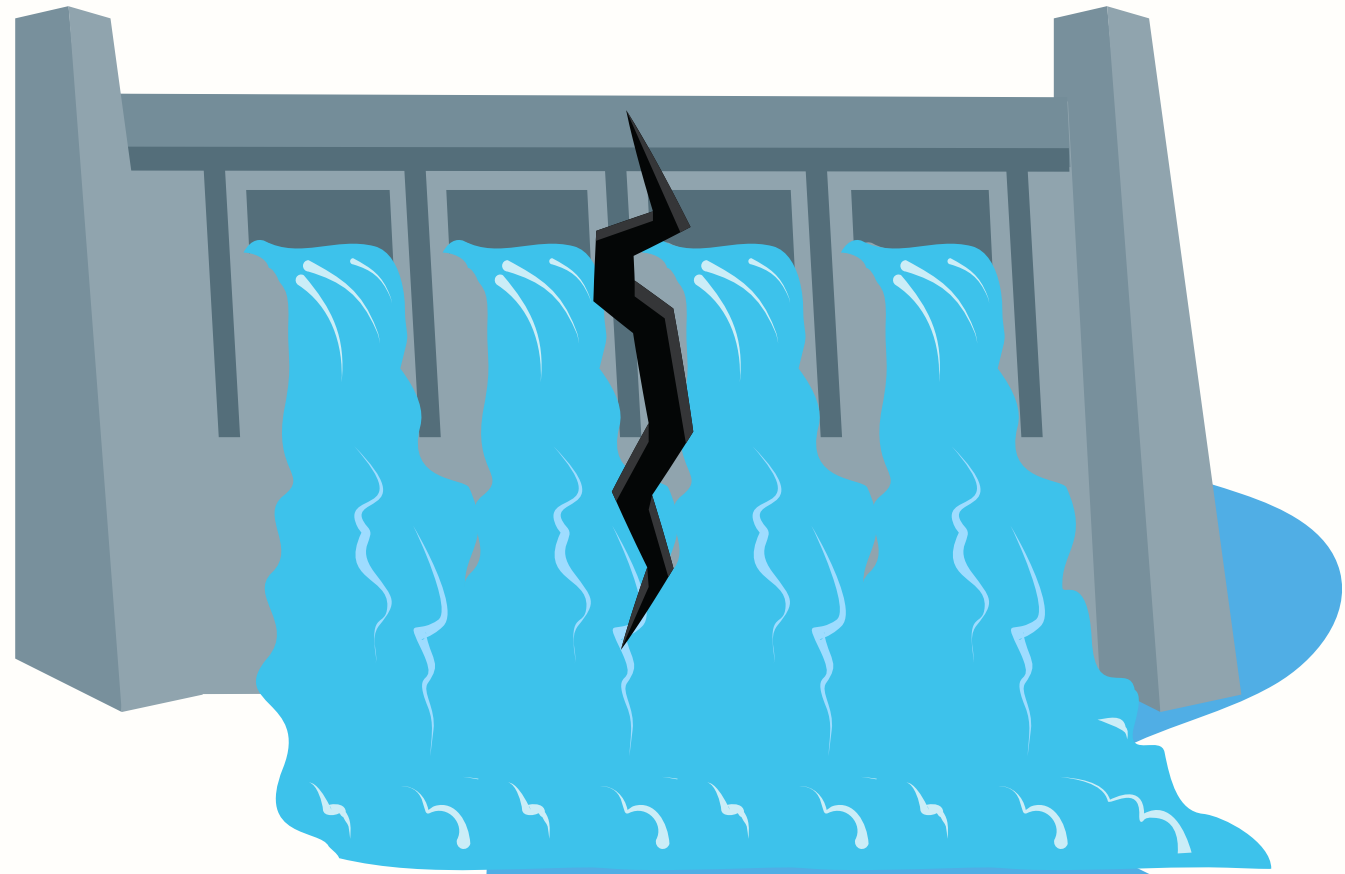
British Museum worker sacked over missing treasures

16 August





**THREAT**



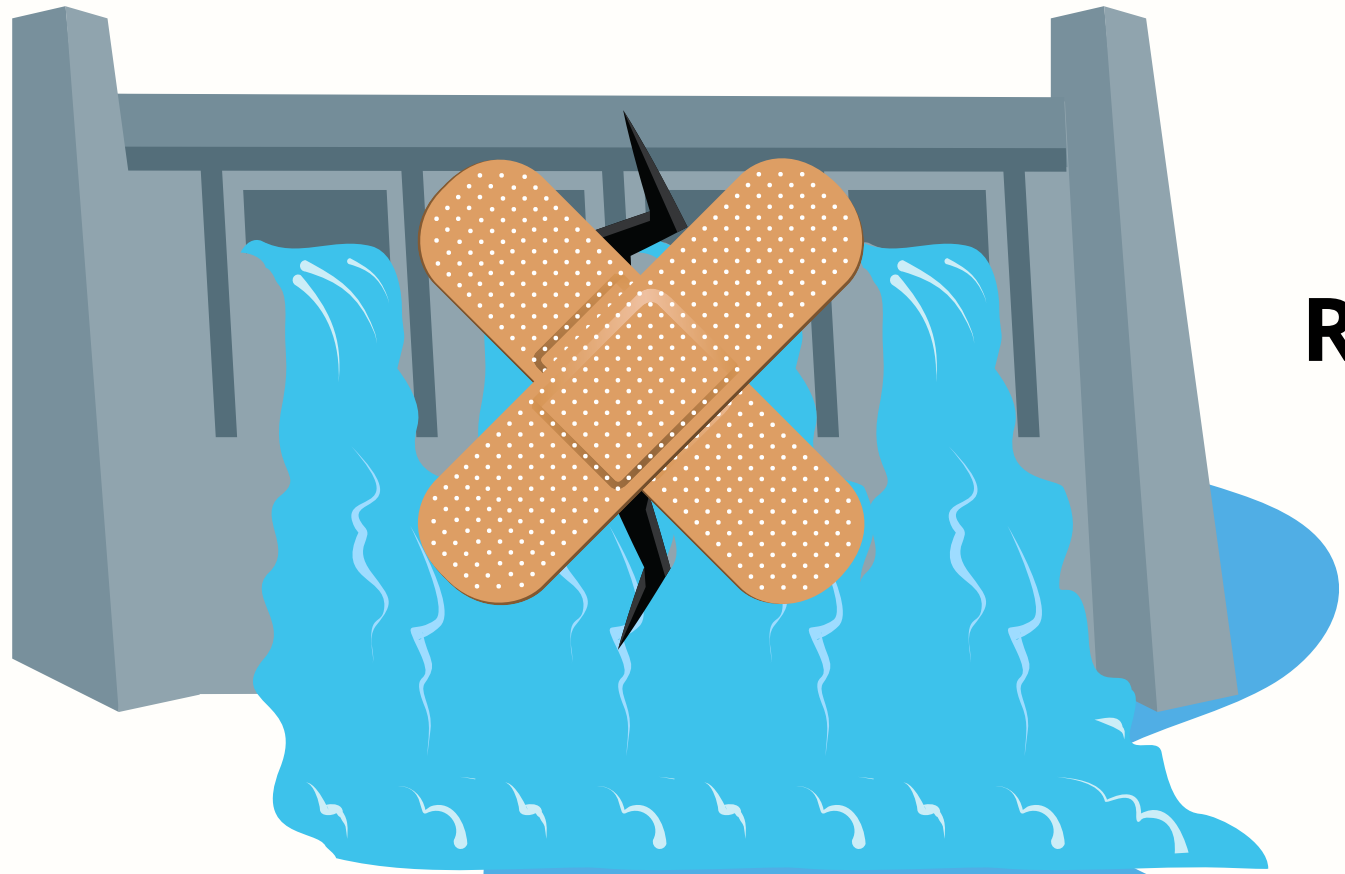
**RISK**

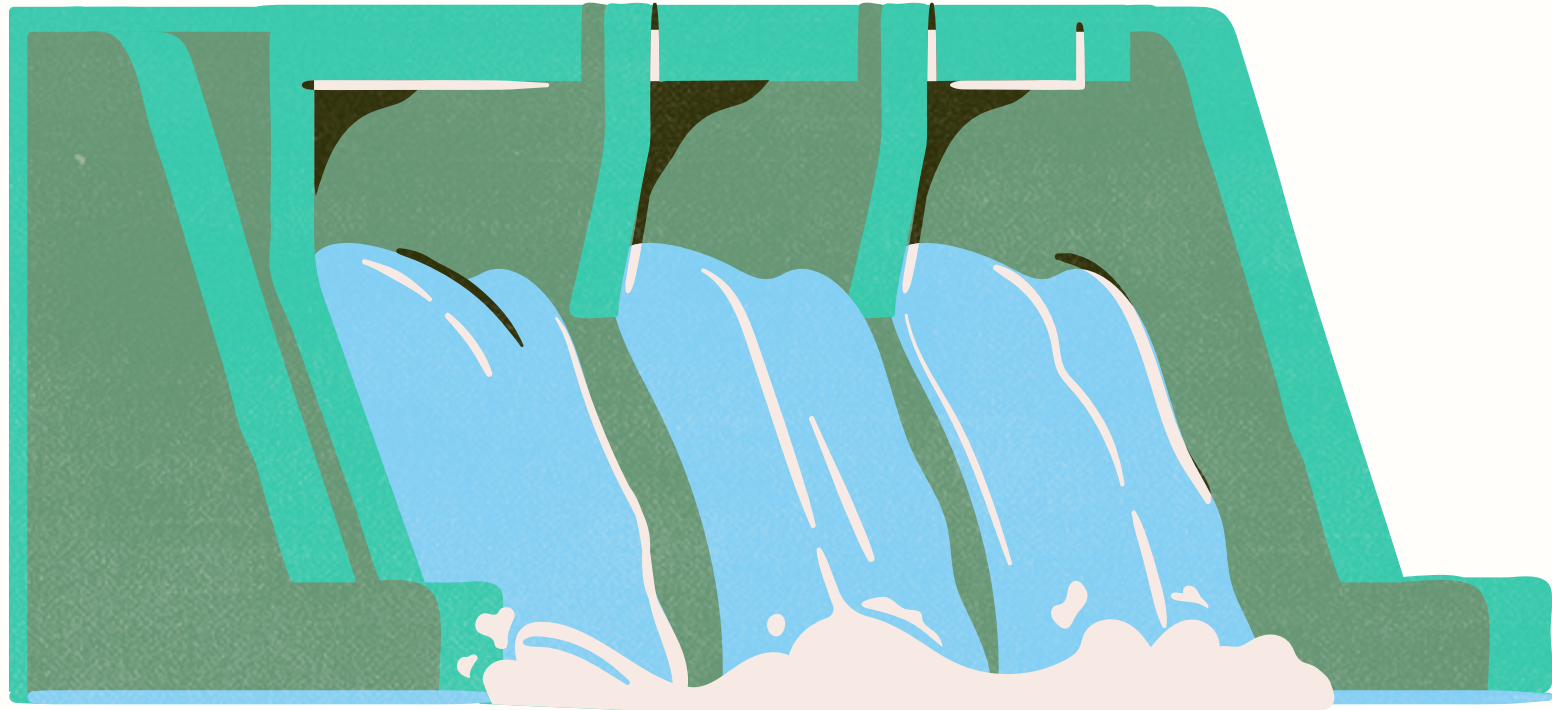


**HARM**



# RISK MANAGEMENT STRATEGY





# RISK MANAGEMENT STRATEGY



# SHARING INFO VIA EMAIL & TEXTS
















- **PDFs + images easily altered by others**
- **Can be reshared without your knowledge**
- **Most hacked method of communication**

**DID YOU KNOW?**

**Using unsecure methods and  
tools puts insurance claims at risk**

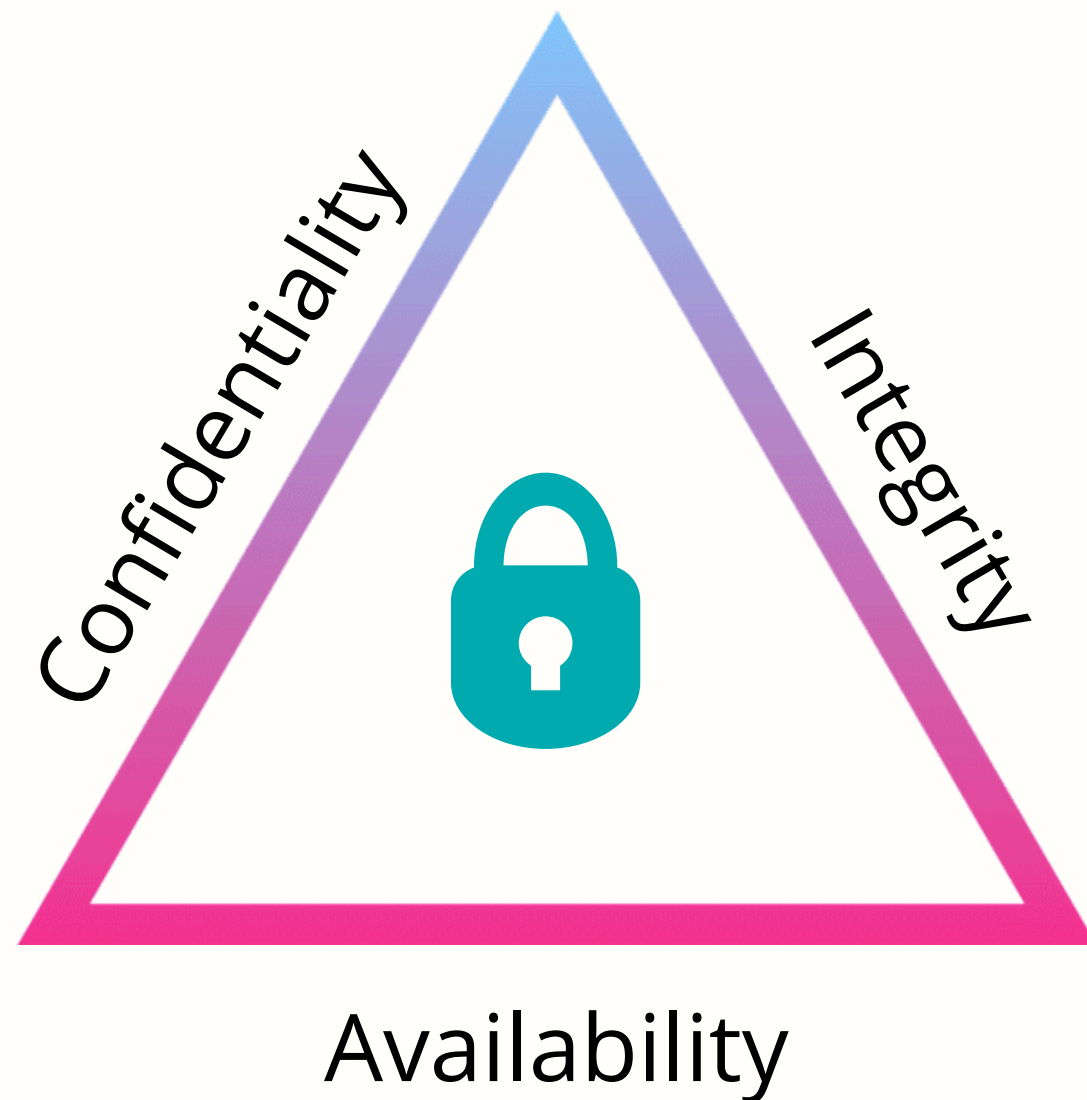


Security Concern	Why does it matter?		 <b>WhatsApp</b> (owned by Facebook)	 <b>Zoom</b> (sells data to Facebook)	<b>Email</b> 
<b>2-Factor Authentication</b> for sender and receiver	<i>Mass password breaches e.g. Facebook: 2013, 2014, 2019 x4, 2021 (half billion users)</i>	<input checked="" type="checkbox"/> Required for all users			
<b>Authorized Sharing</b>	<i>Location and value of works should never be shared outside of authorized parties.</i>	<input checked="" type="checkbox"/> Closed system sharing via custom link that can only be opened by the intended recipient	 Can be shared with anyone	 Can be shared with anyone	 Can be shared with anyone
<b>Data Ownership</b>	<i>Sensitive data needs to be owned and controlled by lending institution or responsible party.</i>	<input checked="" type="checkbox"/> Client data remains property of client as per Articheck T&Cs	 Data shared with Facebook and third parties	 Data shared with third parties e.g. Zoom selling to FB	 Lack of clarity

# WHAT CAN I DO RIGHT NOW?



# 1. Send Sensitive Data Securely



- Email and texts are the most easily hacked forms of communication
- Emails can be forwarded on to unknown recipients
- Content can be changed/manipulated once sent, e.g. PDFs
- Information can be taken out of context



# How To Send Sensitive Data Securely

Sometimes you have to let go of perceived control to improve security



**AUTHENTICATION & ACCESS  
USING THE CLOUD**

# 2. Use 2FA - Two Factor Authentication



- Usernames + passwords can easily be hacked
- Easily memorizable passwords are unsecure e.g. Password1
- Reusing passwords across accounts/websites compromises security of all

# 3. Keeping Software Updated



- Hackers are always working and coming up with new ways to attack
- New software developments and improvements can prevent attacks in new ways
- Usability of software – app vulnerabilities are a way in for hackers

# 4. Hardware Best Practices



- Password protection & screen timeouts
- Consider replacing devices – OS of old hardware can't be updated
- Regular backups – physical hardware can be lost
- Decommissioned devices contain sensitive info

# 5. Encourage Employee Education



- Employees are often the first to see/interact with threats = first line of defence
- Majority of breaches caused by human error
- Understanding threats encourages responsibility/action

# 5. Encourage Employee Education



- Training + teaching to spot suspicious activity e.g. phishing emails
- Reinforce best practices e.g. enforce password changes, lowest permission level when sharing data.
- Write a company security policy, start with 1 page, use this presentation as a reference!

# Thank you!

Questions?

Contact us: [hello@artichheck.com](mailto:hello@artichheck.com)

