SAGESSE

ISSN 2560-7014

SAY GOODBYE TO MAY LONG WEEKEND

Mark Grysiuk, C|CISO, CRM, CIP

ABSTRACT

SAY GOODBYE TO MAY LONG WEEKEND is a fictional case study about a Canadian organization attacked by hackers right before May long weekend. All their core systems go down. The Records Manager plays a critical role in guiding management decisions and providing insights into incident response planning. What happens next after the first two hours? Readers can draw their own conclusions.

What bad timing. It is 3:30 on a Friday before the May long weekend when your phone rings. Just let it go to voicemail. Thinking about this weekend's wine tour in Niagara region, four o'clock pm cannot come fast enough, you mutter quietly. The COVID-19 pandemic officially ended last month. This is your first vacation in two years.

It rings again, and then again. You fight the urge to pick up the phone.

Against the advice of your intuition, you check your voice messages.

It is your IT manager, Jamie. She thinks there has been a breach. All systems are down. You have been asked to attend a meeting in one hour to provide an update and discuss next steps. You have been asked because senior management believes you are the most qualified to advise and protect the integrity of your organization's efforts to *document* and *contain* the breach.

Wow, as your mind drifts away, absorbing what had just happened, that presentation you gave to the Board six months ago about ARMA International's Generally Accepted Record-

keeping Principles[i] must have resonated with management, specifically The Principle of Availability and Integrity.

Drifting off in thought. Wondering what you will say to your close friends who have been looking forward to this short weekend getaway.

You can hear it now,

“Rob, what do you mean you are cancelling on us? You have been with this company for three years and haven’t taken a break.”

And you respond with,

“I don’t want to lose my job.”

Cutting you off in mid-sentence, your friend Joey responds with,

“You won’t lose your job. You are like, one of the best at what you do, and are always getting job offers. Get over it!!”

Reality sets in.

You and your IT services team have known for some time now about the vulnerabilities impacting your web application systems.

In fact, a recent external audit discovered one of your organization’s web applications exposes sensitive information in error messages that is easily missed but quite visible if you are looking for it. This, you recently learned, is a common issue with applications that are not properly configured. You look through the window of the meeting room across from your desk where the meeting will be taking place, and can see a poster on the wall displaying OWASP top ten web vulnerabilities[ii]. OWASP (Open Web Application Security Project ®) refers to this as the Security Misconfiguration Risk[iii].

And an older app containing personal health information, which should have been decommissioned three years ago, is vulnerable to what OWASP refers to as the Broken Access Control[iv] security risk.

---

[i] Generally Accepted Recordkeeping Principles (https://www.arma.org/page/principles)
[ii] OWASP top ten web vulnerabilities (https://owasp.org/www-project-top-ten/)
[iii] Security Misconfiguration Risk (https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration)
[iv] Broken Access Control (https://owasp.org/www-community/Broken_Access_Control)

The auditor pointed out that an attacker could exploit these flaws and gain access to personal information in user accounts and/or conduct reconnaissance to execute a ransomware[v] attack.

Observing the time, forty-five minutes until the meeting starts. Your mind wanders to past conferences and webinars, and all the meetings talking about what must happen to mitigate the risk of a security incident that impacts availability and integrity of your systems.

Looking out the window, a white Ford van has been parked in the school parking lot for several hours.

Outside, many of your colleagues are leaving the office. At the high school across the street, teenagers are rushing outside. Spring is in the air. The sun shines. The April showers have brought beautiful May flowers, blooming in the gentle breeze, lightly brushing against the trees tucked in the valley that overlooks your office building. The partially clouded sky signals the beginning of a beautiful long weekend.

But not for you…

Expect a long weekend, pounding back coffee and eating pizza.

Thirty minutes until everyone arrives.

Earlier this year you and your IT Manager convinced management that it would be a good idea to follow a security standard. Given your organization's size and home base in Canada, you have chosen the Canadian Centre for Cybersecurity's Baseline Cyber Security Controls[vi] for Small and Medium Organizations. Management agrees with the idea but had yet to commit to annual funding of the program.

But now, none of the past narrative matters.

As the clock ticks towards 5:00 pm, your mind branches like a spider spinning its web in several directions.

What are your next steps? Do you call the Privacy Commissioner? Do you call a lawyer?

---

[v] Ransomware (https://en.wikipedia.org/wiki/Ransomware)
[vi] Canadian Centre for Cybersecurity's Baseline Cyber Security Controls (https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations)

With a plan, you would know exactly who to call first. You would know whether you should be preparing a website to address questions from the public or whether you can utilize a different response strategy. More importantly, you would feel confident that your response aligns with generally accepted security response best practices.

Not like Equifax's response in 2017[vii]:

Equifax's Management created a site called 'equifaxsecurity2017.com' directing consumers to enter the last six digits of their social security number to determine if they have "potentially been impacted." How could an organization with so much personal information even consider that type of response?[viii] Thinking about it, one that was not prepared. A security researcher created an almost identical site called "securityequifax2017.com," demonstrating how easy it would be to fool consumers.

Flipping through your notes, a phone number appears. Next to that phone number is the name of a lawyer who specializes in privacy breaches and technology law, and a note stating, "highly recommended." Without thinking, you dial the number. The lawyer picks up after two rings. The lawyer agrees to meet with management tonight at 6 PM.

Retrieving your notes from last week's presentation by Cybersecure Canada Certification Body is the next step to prepare for the meeting at 5:00.

Looking at the first page, Cybersecure Canada's Information Sheet[ix], at the top of the page,

To achieve certification, "…your organization must review and implement the 13 security controls established by the Canadian Centre for Cyber Security."

And the first step is to have a plan.

That plan, according to last week's presenter, Victor Beitner, "should address incidents ranging from trivial to extremely severe, including incidents that cannot be handled directly by the organization."

You are also aware that, even before incident response can be effective, your organization will need to undergo a comprehensive compilation of its system assets. In cybersecurity, identifying all critical information systems is critical. Not ninety percent of systems, one

[vii] Equifax's response in 2017 (https://archive.epic.org/privacy/data-breach/equifax/)
[viii] How could an organization with so much personal information even consider that type of response? (https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/)
[ix] Cybersecure Canada's Information Sheet (https://www.ic.gc.ca/eic/site/137.nsf/vwapj/cybersecure-info-e.pdf/$file/cybersecure-info-e.pdf)

hundred percent, because ninety percent means ten percent of your Crown Jewels are vulnerable to an attack.[x]

Often referred to as a system inventory/data map, it must identify all applications and systems, servers, software, and their respective versions, and system value (i.e., extremely sensitive equals high impact). Your IT department purchased a configuration management database[xi], but it lacks a dedicated resource. Patch management, which is a core requirement to mitigate IT system risks, can be effectively managed using a well-resourced configuration management system. This system will help your organization identify risks, assign owners to those risks, and develop risk mitigation strategies.

Continuing, you review the section of your notes, based on the preparation, identification, eradication, recovery, lessons learned incident response framework.

PREPARATION[xii]

It should not be any surprise that training staff on how to respond, and/or whether they are directly involved in incident response is key requirement for preparation. It would be expected that on an ongoing basis, you will be preparing your staff on how to identify and respond to different incidents. In addition to mandatory training, offering workshops, writing newsletters, and sending reminder emails to key staff will help in the preparation stage.

With leadership support, following Baseline Cyber Security Controls for Small and Medium Organizations[xiii] will guide your organization's implementation. Identify and designate all staff required to manage cybersecurity incidents, including responding to external parties and defining their roles and responsibilities. For example, if the organization does not have a legal department, the records manager can be the designated staff member to initiate all contact with outside counsel and regulators (i.e., your province's privacy commissioner if you have one). Consider designating as a second contact your IT manager, who may be better positioned to adequately describe the details to outside counsel when required on short notice. Contact list should include employee name, job title, contact information.

If internal resources cannot commit to what could be calls early in the morning or late at night, engage a third-party service provider to support your organization outside regular business hours. That third-party service must have the authority to initiate incident response procedures.

---

[x] Cybersecurity experts always advise organizations to inventory *all* their information assets. The concept presented as, "Not ninety percent of systems, one hundred percent," comes from Eric Cole, author of Cyber Crisis: Protecting Your Business from Real Threats in the Virtual World.
[xi] Configuration management database (https://www.youtube.com/watch?app=desktop&v=on_41LX7cas)
[xii] https://www.securitymetrics.com/blog/6-phases-incident-response-plan
[xiii] Baseline Cyber Security Controls for Small and Medium Organizations (https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations#a31)

Developing user stories are more engaging to non-technical users and will help them understand the impact of low, medium, and high-risk incidents. User stories provide valuable insights on how to handle, for example, a ransomware attack, a phishing email, or a document sent to an incorrect email address (for some examples see appendix). Scenario-based learning should be part of all training and awareness activities.

Ideally, however, there should be a small number of staff that can step up if required. Not meeting this minimum requirement means the organization will not receive credit for Baseline Control BC 1.1[xiv]. Flag this is as a high risk and assign an owner it. It must be a senior leader, preferably the most senior person.

Purchasing cybersecurity insurance is Baseline Control 1.3 (BC 1.3)[xv]. Check with your current insurance provider. The organization may already have some coverage. If required, consider expanding that coverage. Insurance companies can also recommend preferred third-party forensic service providers, as well as privacy breach coaches. Add all this information to the written plan.

How far do you need to go with training? How specific do the examples need to be in the training and what are we learning objectives? See the next section.

IDENTIFICATION

Every employee within your organization should be able to identify when or if an incident is taking place. And they should not be afraid to report an incident[xvi]. They do not need technical knowledge but there should be a plan in place to proactively educate on how to spot and report red flags, including:

- Unauthorized use or access (e.g., a lagging computer when there are no planned software updates could indicate that a cryptojacking attack[xvii] is underway.)

- Service interruption or what is sometimes referred to as denial of service. (e.g., your email account is bombarded with thousands of email messages, or your website crashes due to the volume of unanticipated activity)

[xiv] Baseline Control BC 1.1 (https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations#a31)
[xv] Baseline Control 1.3 (BC 1.3) (https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations#a31)
[xvi] They should not be afraid to report an incident (https://www.linkedin.com/pulse/why-good-idea-promote-culture-fear-mark-grysiuk-cciso-crm-cip/)
[xvii] Cryptojacking attack (https://www.investopedia.com/terms/c/cryptojacking.asp)

- Malicious code (e.g., ransomware software that encrypts all your information, and your organization's information is then controlled by a bad actor)

- Network system failures (e.g., The denial of service mentioned above is likely to lead to an enterprise-wide system failure if not contained quickly)

- Application system failures (e.g., new software functionality that has not been properly tested and contains vulnerabilities that leads to application system failures.)

- Unauthorized disclosure or loss of information

- And, yes, whether a breach is underway.

Some of this can be done with technology depending on your budget. Simulated phishing campaigns executed monthly are very effective in helping employees spot bad emails. They help remind staff that just because a URL uses the HTTPS protocol, does not mean that it is safe, and that very subtle spelling errors can easily be missed (e.g., a missing letter in a domain name). Of course, there is more to it than just sending out a monthly phishing test. Establish a baseline metric after the first test. Over the next twelve months, assign training as required, and keep track of who requires customized support. Expect the click rate to trend downward, assuming training is well-received by staff.

While employees do not require technical skills, they should have the skills to quickly capture error messages in a screenshot. This helps IT be more effective in diagnosing and resolving issues, especially those related to application system failures. (Don't assume all your staff know how to take screen shots.)

CONTAINMENT

The National Standards Institute of Technology[xviii] advises that "an essential part of containment is decision-making." When is it appropriate to, for example, shut down a system, disconnect it from the internet, or disable certain functions? [xix]

When an incident takes place, report it to your helpdesk and/or incident response team, the appropriate designated employees will take immediate action to contain the incident. Their activities include but are not limited to isolating the incident, determining the source and where it came from and what vulnerability the unauthorized intruder exploited, resolve any

[xviii] National Standards Institute of Technology (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
[xix] 3.3.1 Choosing a Containment Strategy

identified vulnerabilities, and continuously assess the damage and impact. What is most important is acquiring, preserving, securing, and documenting evidence and preserving chain of custody.

Also, remember to treat IT and security resources with respect. Providing breakfast, lunch, and dinner at no cost to the team is highly recommended. Stress levels will be high and any moral support that can be provided will be greatly appreciated.

ERADICATION

Depending on the severity of the incident, and the resources that have been deployed, some time may go by before you begin the eradication step. This is when all traces of the infection have been removed from systems. Vulnerabilities will be identified and, ideally the forensic experts will have determined the root cause of the incident, removing malware, viruses and any other dysfunctional code that contributed to the system breakdown. This step will also include identifying all impacted devices and removing them from the environment.

RECOVERY

At this stage, hopefully within the first twenty-four hours of the incident taking place but could be longer depending on the severity of the incident, your incident response team will be taking the required steps to recover. Assuming your organization has a disaster recovery plan, which prioritizes your systems in accordance to value, your incident response team will return those systems back to an operational state by order of priority utilizing the most recent backups.

While this is going on the incident response team will be monitoring the systems as they are brought online and assessing in real time as to whether the incident may reoccur. They will also be making sure that the systems are restored from a clean source. And they will be confirming that all impacted systems are functioning as they are intended to function. Additional monitoring may continue to look for related activity if it is deemed necessary.

LESSONS LEARNED

While this may be obvious, it is crucial that organizations examine its existing processes and develop an ongoing mitigation plan to reduce the likelihood of a similar incident reoccurring in the future. Do not wait too long after an incident has been resolved to conduct this final step. Crucial perspectives from the varying stakeholders involved will be lost.

Sitting in your desk, looking out your window while pondering everything in your notes, that white van still idles, alone in the parking lot, now covered in shade from the valley above.

At 4:57, a text message from IT reporting that the entire team is in the containment stage, disconnecting systems from the network but not disconnecting power.

The management team arrives together at 5:00. The meeting begins. The CEO, looks at you, and asks,

“Robert, what happened?”

To which you succinctly reply,

“We are under what looks to be a malware attack. Our core systems are down. We are not able to provide an exact cause at this time and whether any sensitive information has been exposed.

IT will be working through the weekend and will have an update at 8:00 pm tonight. I have also engaged outside council. Their team will meet with us at 6:00 pm. I highly recommend we follow their advice before making any formal announcements.”

“Robert, what are we not doing that we should have been doing?

“I am not hear to cast blame, but it has taken far too long to address the vulnerabilities flagged during the last audit. Rather than focusing on the past, let us learn from our mistakes. We can talk about approving our funding request next week. Right now, we, and by we, I mean the entire information management team, would ask that the room where IT is currently working be sanctioned off. We need to remove all people not involved in this incident. If there’s anyone left on the floor please ask them to leave immediately. We cannot risk unauthorized staff tampering with any evidence.”

We do not need your entire team here all weekend, but you should be available for updates and decisions. My recommendation is to follow the advice of counsel. I have cancelled my weekend plans and will be staying late.

FINAL THOUGHTS

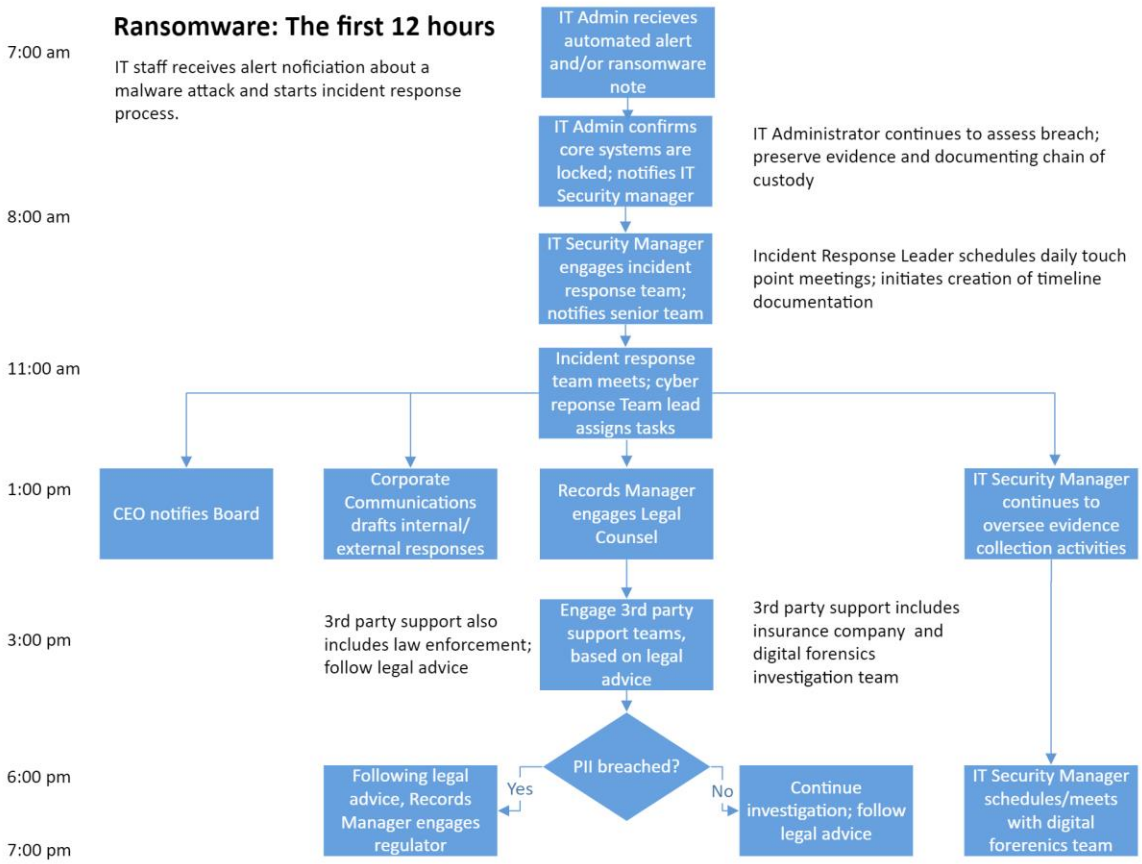
If you are currently under attack, do not overreact. Stay calm.
Engage legal counsel and follow their advice.
If you do not have legal counsel, conduct an online search. Finding a reputable firm quickly should be relatively easy.

If you are not under attack and do not have legal counsel, you are one step behind everyone else. Step up and engage, before it is too late.
And that van in the parking lot that no one is thinking seriously about…. I will let the reader draw their own conclusions.

ABOUT THE AUTHOR

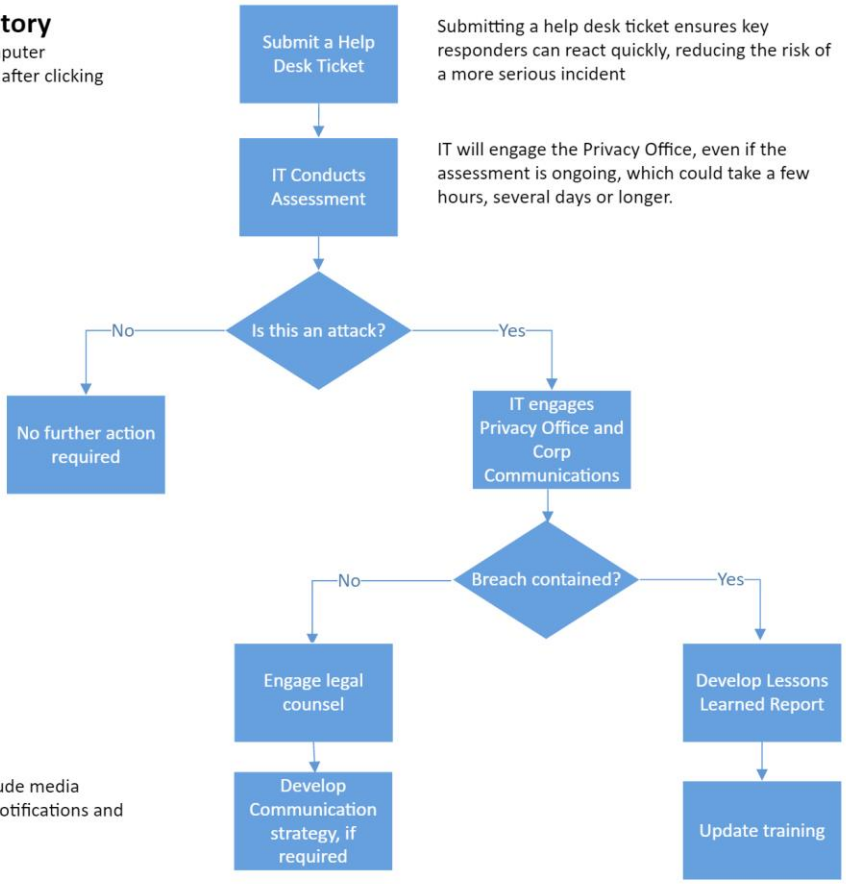
Mark Grysiuk has been working as an information management practitioner for 18 years. He is a Certified Chief Information Security Officer, Certified Records Manager and Certified Information Professional. Mark won ARMA's 2015 Brit Literary Award for an article entitled The Cookie trail: Why [Information Governance] Pros Must Follow the Crumbs.

Appendix


Ransomware: The first 12 hours
7:00 am
IT staff receives alert nofication about a malware attack and starts incident response process.
IT Admin recieves automated alert and/or ransomware note
IT Admin confirms core systems are locked; notifies IT Security manager
IT Administrator continues to assess breach; preserve evidence and documenting chain of custody
8:00 am
IT Security Manager engages incident response team; notifies senior team
Incident Response Leader schedules daily touch point meetings; initiates creation of timeline documentation
11:00 am
Incident response team meets; cyber reponse Team lead assigns tasks
1:00 pm
CEO notifies Board
Corporate Communications drafts internal/ external responses
Records Manager engages Legal Counsel
IT Security Manager continues to oversee evidence collection activities
3:00 pm
3rd party support also includes law enforcement; follow legal advice
Engage 3rd party support teams, based on legal advice
3rd party support includes insurance company and digital forensics investigation team
6:00 pm
PII breached?
Yes
No
Following legal advice, Records Manager engages regulator
Continue investigation; follow legal advice
IT Security Manager schedules/meets with digital forerenics team
7:00 pm

Phishing Attack User Story

Employee observes his or her computer operating really slow not too long after clicking on a link.



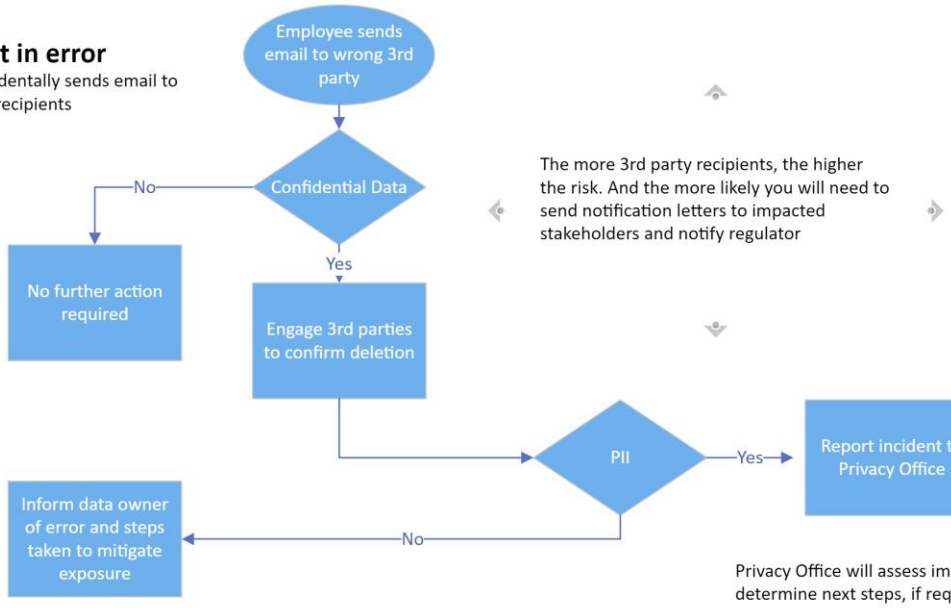
Submitting a help desk ticket ensures key responders can react quickly, reducing the risk of a more serious incident

IT will engage the Privacy Office, even if the assessment is ongoing, which could take a few hours, several days or longer.

Communication strategy may include media release, community stakeholder notifications and FAQs, subject to legal advice

Email sent in error

Employee accidentally sends email to unauthorized recipients



The more 3rd party recipients, the higher the risk. And the more likely you will need to send notification letters to impacted stakeholders and notify regulator

Privacy Office will assess impact and determine next steps, if required

Data owner will determine whether additional steps are required