Data Breach –
A “First Response” Legal Playbook

OVERVIEW: *Cyber-attacks and data theft incidents continue be top of the risk register and threat actors’ tactics and operating models are becoming increasingly sophisticated. Accordingly, data breach response preparedness is vital for in-house lawyers.*

*This presentation focuses on the **initial 72 hours** – the “first response” stage – and offers a playbook for in-house legal teams.*

Presenters:
Stephen H. Baird – Associate General Counsel at SITA
Simon Elliott – Partner at Dentons

January 2024

Disclaimer:

The views expressed during this program do not constitute legal advice, belong solely to the panelists, and do not reflect the views of the Association of Corporate Counsel or the entities for whom the panelists are employed.

Agenda & Introduction

I. The **Global Digital Context**

II. The **Threat Context** – *“Not if, but when?”*

III. **Data Breach Response** – “Executive Playbook” for first 72 Hours

IV. **Lessons and Next Steps**

V. **Discussion, Questions** and Close

Introduction – Presenters

Stephen H. Baird is Associate General Counsel at **SITA** (www.sita.aero), the world's leading specialist in air transport communications and information technology. SITA serves over 200 countries and territories. Stephen graduated from the University of Western Australia's Law School and has 25+ years experience. For SITA he leads on legal issues relating to product technology, data, partnerships and innovation. He is based in Geneva, Switzerland.

Simon Elliott is a Partner at the law firm **Dentons** and leads its market-leading UKIME Data Privacy and Cyber Security group. He has 15 years+ experience as an expert advising clients on the full range of data privacy and cyber matters including leading large-scale global projects designing and implementing global privacy frameworks and strategies as well as supporting on the operationalization of privacy programs within organizations. Simon also regularly assists major global multi-nationals and UK businesses with regulatory investigations and enforcement actions by privacy regulators, supports on the increasing flow of data protection litigation and media enquiries focusing on privacy practices. Simon is identified as a "Next Generation Partner" by The Legal 500 for data protection, privacy and cybersecurity and is a Ranked Lawyer in Chambers for "Data Protection & Information Law".

I. The Global Digital Context

The Global Digital Context (1 of 2)

- Our society and commerce depends on digital operations. Data is the fuel for the progression of our technological advances - e.g. AI.

- Technology is becoming more complex as legacy systems remain operational and patching becomes more urgent. Technical security debt continues to increase – speed to market undermining security.

- Budgets for cyber defense will always have constraints.

- There is not always alignment between database size & sensitivity and defenses in place.

The Global Digital Context (2 of 2)

- The data and digital regulatory environment continues to expand and increase in complexity.
- New and more comprehensive data privacy and information security laws reflect the societal importance of data and data infrastructure.
- This is increasing the regulatory risk associated with data breaches.
- And insurers are becoming more wary of cyber risks.

II. The Threat Context

The Threat Context (1 of 3)

- Threat actors' tactics and operating models are becoming increasingly sophisticated. Nation-states and groups powered by AI and the professionalization of dark market for services.

- The human/employee threat vector & 3rd party supply chain remains as much of a risk as the technology.

- Many industries are specific targets – technology, utility, manufacturing, government, banking, health, travel, education, professional services among others. Recently even libraries and cities …

  October-December 2023 – British Library: https://www.newyorker.com/news/letter-from-the-uk/the-disturbing-impact-of-the-cyberattack-at-the-british-library
  January 2024 – Majorca, Spain: https://www.bleepingcomputer.com/news/security/majorca-city-calvi-extorted-for-11m-in-ransomware-attack

- Successful attacks can cause serious threats to business continuity and significant loss.

The Threat Context (2 of 3)

- Zero Day attacks are becoming more common.
  - *"Zero Day" refers to a security vulnerability that hackers can use to attack systems which the vendor or developer is unaware of – and therefore no patch or specific defense exists for the vulnerability.*

- Ransomware continues as a key threat but is evolving into double and triple extortion attacks (encrypt; exfiltrate; harass). Credential stuffing attacks also a significant recent trend.

- A single attack can use multiple Zero Days, especially if performed by a nation-state actor. The increasingly difficult geo-political landscape adds a further dynamic to cyber risks.

- Governments are recognizing the threats. E.g. Japan is significantly increasing the size and training for its cyber defense unit from around 900 staff in 2023 to 4,000 by 2027.

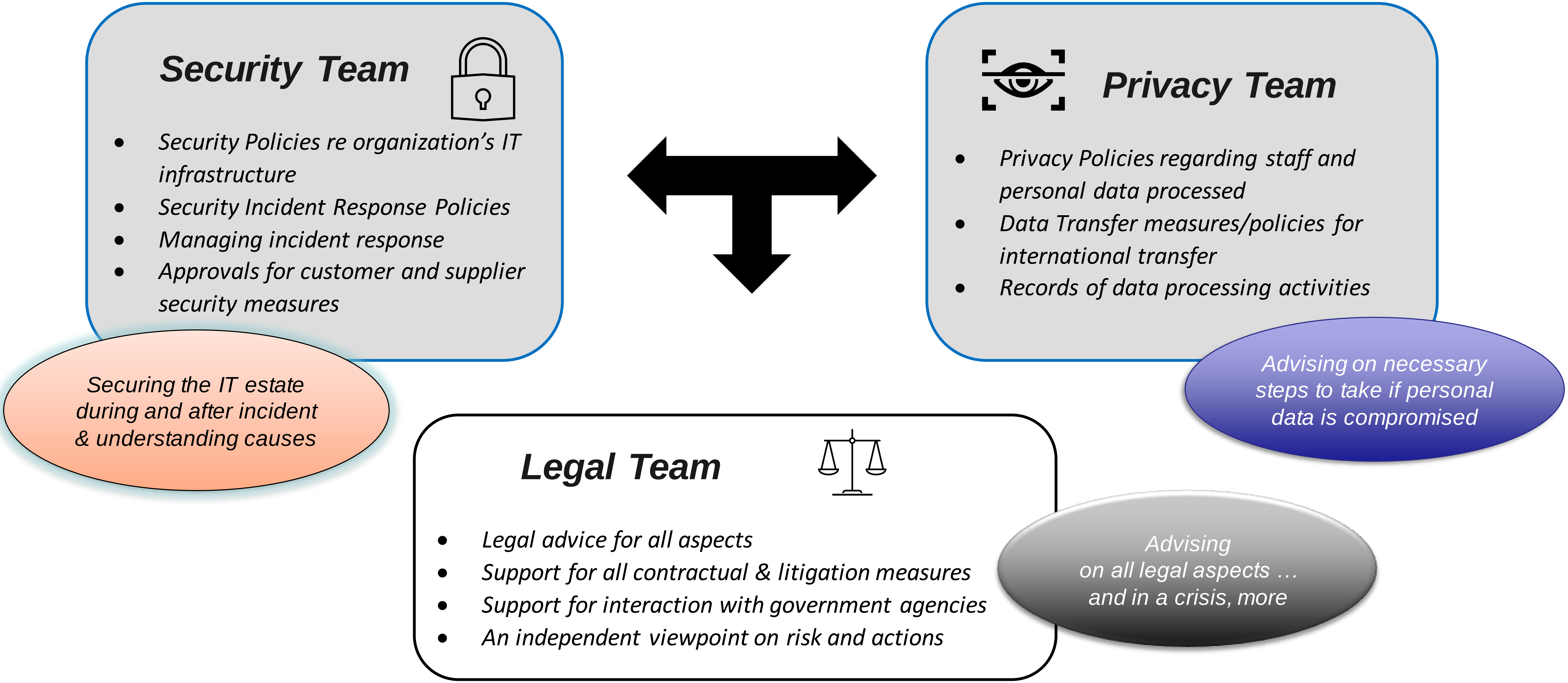
Source: https://www.japantimes.co.jp/news/2023/07/11/national/sdf-cyber-capabilities/

The Threat Context (3 of 3)

- The emerging trend is for broader information sharing of attack vectors and origins in a collaborative manner.
- Balanced data sharing may benefit individual organizations and can contribute to societal resilience against cyber threats.
- For example, the *International Counter Ransomware Initiative* (CRI), now with 50 member countries, stated in November 2023 that it plans to launch information-sharing platforms enabling CRI member countries to rapidly share threat indicators.

  Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/
- Question of ransom payment remains a complex and risky assessment.

Roles & Teams



Security Team

- Security Policies re organization's IT infrastructure
- Security Incident Response Policies
- Managing incident response
- Approvals for customer and supplier security measures

Securing the IT estate during and after incident & understanding causes

Privacy Team

- Privacy Policies regarding staff and personal data processed
- Data Transfer measures/policies for international transfer
- Records of data processing activities

Advising on necessary steps to take if personal data is compromised

Legal Team

- Legal advice for all aspects
- Support for all contractual & litigation measures
- Support for interaction with government agencies
- An independent viewpoint on risk and actions

Advising on all legal aspects … and in a crisis, more

III. Data Breach Response

A Legal Executive Playbook for the first 72 hours

Data Breach!

- The first 48-72 hours is a vital time period after discovery of any cyber-attack on your organisation that may involve personal data or critical data.
- If your organization is unfortunately targeted, the following is suggested as a practical list or "playbook" at Executive level for actions.
- Each situation will be unique and involve different stakeholders, customers and/or suppliers.
- As always: Preparedness is key

You will get a call – it could be at any time. (Probably when you are on holiday)

The person will say:

Hi ! Good Day !

So – we might have a problem …

We are checking, but we may have had a hacker inside our IT systems.

… it could be bad, but we hope not …

Don’t worry – the IT teams are working on it. We will keep you in the loop!

And later:

Actually we found out it’s bad … it’s been ongoing for some days – or months …

Hour by Hour – the Vital Steps

1. **0-6H: Chain of Command**
   - Build the Machine
   - Minutes & Resources
   - Know & follow policies
2. **0-48H: Exercise Caution**
   - Questions to ask Technical Leads
   - Legal Privilege
   - Board & Senior Management Communications
3. **12-72H: Prepare Notifications ASAP**
   - Govt Regulators & Law Enforcement
   - Stakeholders/Customers
   - Banks / Credit Card issuers
4. **Publicity & Crisis Communications**
5. **Cost assessments**

1. Chain of Command: 0 to 6 Hours

"Build the Machine" (You may need to build it, if it's not rehearsed & ready.)

- Confirm who leads what, the response team structure, roles & responsibilities, meetings and communication lines.
- Ensure the right skill-sets are represented on the relevant committees and decision-making teams.
- Consider the human impact – preparations for managing and supporting core team members who will be physically and mentally stretched for an extended period.

> *Minutes and Resources*

This will become important later.

- Immediately start minuting all meetings from the get-go. Maintain a clear record of managers’ involvement.
- You will need resources – including admin resources – for tracking all meetings and decisions made.
- Track and log risk items, mitigants and ongoing issues.

> Policies – Follow them

Does your organization have a specific confidential process for determining ransomware response?

The question will come up:

- Did you follow your Crisis Policies?
- Minute that you are following your policies or if deviating, make sure that this is also minuted with the reasons.
- E.g. If the policies say that Head of IT Security is to chair meetings, make sure that occurs.

2. Exercise Caution: 0 to 48 hours

- The investigation will be ongoing and things you thought were “facts” may change. E.g. hacker **may still be inside networks**, even if teams thought not.
- Be a “devil’s advocate” for the worst case scenario. Do not rush to judgement about the scale of the issue – it may be worse than expected.
- Be wary of “good news” and know that the full picture might take time to emerge.

> *Questions to ask Technical Leads*

- *Is the event ongoing? Is it contained?*
- *Is the threat actor still within the business environment?*
- *Is a view of accessed / exported data emerging?*
- *Is the cause or access-point known?*
- *Is the scope of compromised assets fully understood?*
- *What is the chain of evidence?*
- *Do we have indicators of external 3rd parties becoming aware (so far)?*

> *Legal Privilege – Use it when justified*

- When engaging external lawyers, be aware of **legal privilege** advantages.
- You likely will want to engage specialist security consultants. Your law firm could engage them to potentially have a stronger privilege position, if loss/harm is anticipated.
- Provide privilege protocols and processes:
  - Clear guidance to internal teams about appropriate terminology and written comms regarding incident; avoid definitive statements of non-compliance and damaging statements.
  - Identify and codify the "privilege club" – who can defensibly receive privileged communications / advice with lawyer copied or included?
  - Establish protocol for security consultants feedback – limit floating drafts of reports; read-out of reports to allow input & comment before finalization.

> *Board and Senior Management Communications*

- Start Board & Senior Management reporting – being **brief, formal reports** that confirm team leadership, organisation and actions.
- Request Board feedback & direction.
- Ensure that reports confirm the application of the company's policies.

3. Prepare & Send Notifications ASAP: 12-72 Hours

- Prepare to advise stakeholders. This may include government agencies, banks, credit card issuers if relevant.
- Consider necessary government regulator notifications. (Even as sub-processor/ contractor it can be mandatory to report to the govt.)
- Consider law enforcement – e.g. cyber-crime divisions.

Full credit card data breach with CVC/CVV numbers – stored not in compliance with PCI DSS standards – can be a "worst case" scenario

> *Legal Requirements re Notifications and Content*

- Laws often mandate that suppliers notify customers “without undue delay” – 72 hours may be maximum time period.

- But regulators now expect impacted parties to notify as soon **as there is a reasonable suspicion of a breach** (as do controllers in contracts with suppliers).

- Content of notifications should short, clear and defensible. It needs to be absolutely correct, and therefore should not “say too much” at this early stage.

- When dealing with high volumes, teams may not be resourced to respond in detail.
  - Consider "broadcast" approach with engagement one-way (i.e. company provides updates).
  - An up-to-date, centralised FAQ may ensure consistency of messaging.

4. *Publicity – Crisis Communications*

- Your Communications/Marketing team will need to prepare a responsive statement & proactive website or other statements.

- Media requesting comment often provide a short window of time (e.g. 1 hour only) before going to press.

- **“Crisis Communications”** may be needed – this is a **specialized area** within media/PR communications.

5. *Costs Assessment*

“How much will this cost us?”

- Be wary of putting a number on the potential loss until the entire incident and stakeholder reaction is known.
- This is likely to take many months.
- If the data breach spans many jurisdictions, a precise loss estimate may be impossible with any certainty.

IV. Lessons & Next Steps

Lessons – Next Steps (1 of 3)

- Organizations must **learn from cyber security incidents**.
- **“Post mortems”** are vital for learning – review what went well and what could be improved.
- Post-incident reviews should be thorough, open and uncompromising about improvement recommendations.
- Acknowledge weaknesses and gaps as **part of continuous improvement**.

Lessons – Next Steps (2 of 3)

- Benchmark your policies & team structures & resources against other similar organizations.

- Test policies, teams & systems with "role-play crisis emergencies".
  - E.g. 3 hour session - complex role-play scenario – with CEO direct-reports participating.
  - Consultants can provide scenarios & "after-action reports" to role-play exercises.

- Make sure everyone knows where to report any strange or unexpected IT events.
  - ➢ Ask them to report **ANYTHING** that seems unusual in IT systems.
  - ➢ They are part of our "eyes & ears".

In IBM's 2022 data security report, it was reported that it took an average of **9 months** for businesses to identify and report a data breach

Lessons – Next Steps (3 of 3)

- Data breaches are becoming more common, meaning advance preparation is more necessary.
- Insurance is becoming harder to obtain.
- Know your policies. Know your amount & type of stored data. Know your suppliers & stakeholders.
- Be ready for surprises.
- If your organization is unfortunate to be a target and the incident is serious, ensuring that the first hours are handed in the most expedient way will support loss mitigation & damage control.

IV. Discussion, Questions and Close

This presentation is supplemented by the ACC Docket article of
12 September 2023 by the authors:
“Data Breach! A Playbook for the First 72 Hours”
https://docket.acc.com/data-breach-playbook-first-72-hours

Contact Info

Stephen H. Baird
Associate General Counsel at SITA (www.sita.aero)
LinkedIn: https://www.linkedin.com/in/stephen-h-baird-9669b019/

Simon Elliott
Partner at Dentons (www.Dentons.com)
Simon's profile: https://www.dentons.com/en/simon-elliott