



- BRENDAN SEATON, SENIOR EDITOR -

Become a Healthcare Columbo: Investigating Security and Privacy Incidents

Brendan Seaton is the President of PRIVA-C, a division of CareLink Incorporated, a consulting firm headquartered in Fredericton, NB that provides a wide range of services focusing on security, privacy and confidentiality issues.

If you are responsible for security and privacy in your organization, you will be called upon to investigate and solve serious breaches. The first rule for dealing with a major security or privacy incident is DON'T PANIC!

Dealing with a major breach often sends the organization into a tailspin, especially if the media is involved. Think of Columbo who, with his disheveled appearance, old car and dog in tow, refused to be rushed or bullied into jumping to quick conclusions or hasty actions. A serious breach of security and privacy demands that calm heads prevail, and that a structured and disciplined approach to investigation take place.

There are as many types of incidents as there are people and things that can go wrong. They include:

- Physical attack such as a violent person in the waiting room, or the theft of equipment or files,
- Logical attack such as a virus infection or hacking attempt,
- The malicious destruction or disclosure of confidential information by a disgruntled employee,
- A natural or man-made catastrophe that brings down a mission-critical system,
- Accidental disclosure of confidential information or destruction of information system assets, and
- Any perceived vulnerability, real or not, that causes concern in the community.

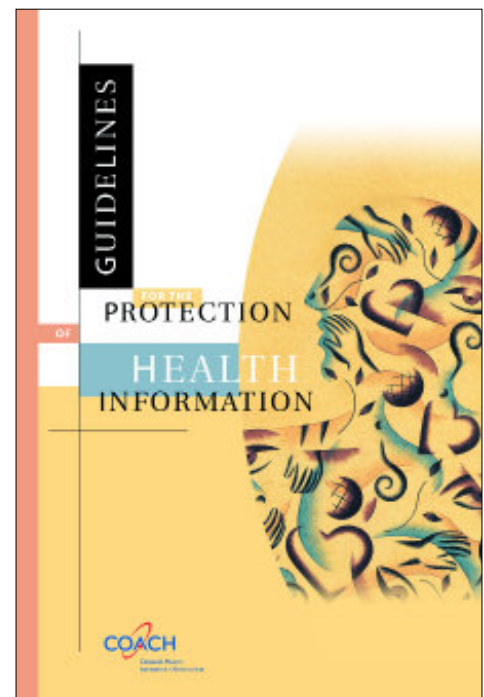


Since 1988, COACH, Canada's Health Informatics Association has provided leadership and guidance in the areas of security, privacy and confidentiality. The 2001 publication gives health informatics professionals the framework needed to develop and implement security and privacy programs. *Guidelines for the Protection of Health Information* reflects the new realities of health informatics as we enter the third millennium and the dawn of the information age.

COACH is proud to offer for purchase the new *Guidelines for the Protection of Health Information*, a valuable reference that no health informatics professional should be without.

Download the order form for the *Guidelines* from the COACH Web site at www.coachorg.com.

COACH, Canada's Health Informatics Association
1304 - 2 Carlton Street
Toronto, Ontario M5B 1J3
Tel: (416) 979-5551
Fax: (416) 979-1144
Toll Free: 1-888-253-8554



The first step in dealing with these and any other incident is to be prepared. There are a few concrete actions you should take in anticipation of an incident.

A common tenet of information security is that 80% of all breaches happen from within. Making sure that your employees are aware of their responsibilities and obligations, training them on the security features of your information systems, promoting privacy enhancing behaviors, and encouraging them to report incidents or suspicious activity is your first line of defense.

It is also necessary to document your efforts in this regard. The first response from an employee accused of a breach is that they didn't know that what they were doing was wrong. The onus is on you to demonstrate that they had every opportunity to be aware of their responsibilities and the consequences of a breach.

While training and awareness mitigates some of the risk, there are some key processes and mechanisms that must be in place. The first is to establish a comprehensive **incident management procedure**. This should be a flexible process that can address a

Ideally, you have conducted a Threat and Risk Assessment (TRA) and have a good idea of the threats to the personal health information you hold, and the vulnerabilities inherent in your systems, processes and people. Forewarned is forearmed. A TRA tells you what to watch for.

So you're prepared. What do you do when an incident actually occurs? You have to move quickly, especially if the incident has just occurred or is in progress. First thing — **GET A NOTEBOOK**. You know the little notebook that the police carry. The one the police officer pulls out in traffic court to prove that he stopped you speeding on the 24th of October at 8:55 pm, when you were going 55 km's over the limit. Or the one Columbo carries that contains a note about a piece of freshly-chewed bubblegum stuck under a table at a crime scene with a tooth mark in it that ultimately traps the killer who had otherwise committed the perfect crime.

It's critical to track the facts, and to **note things as they occur**. In courts and arbitration hearings, original notes taken while the incident or investigation is in progress are often allowed as evidence, whereas reports written after the fact and based on

“A common tenet of information security is that 80% of all breaches happen from within. Making sure that your employees are aware of their responsibilities and obligations, training them on the security features of your information systems, promoting privacy enhancing behaviors, and encouraging them to report incidents or suspicious activity is your first line of defense.”

range of incidents, from minor breaches such as people talking in the elevator, to serious and malicious incidents resulting in the disclosure or destruction of information. The procedure should define criteria for deciding when incidents should be escalated to senior management and when to involve law enforcement agencies. A communications strategy is also part of your incident management procedure, especially dealing with the media.

The second is to establish an **incident response team** to deal with major incidents. The team should include key management personnel who have the authority to investigate and respond to incidents. You should identify external expert resources such as forensic auditors, legal advisors and investigators who can be called in on an “as-needed” basis. The team should establish relationships with law enforcement authorities who may be asked to participate in an investigation, and who can offer useful advice on security preparedness.

The actual people involved in the investigation and response to an incident may vary depending on the circumstances. For example, the information systems group would handle a virus attack, while HR and the employee's managers would manage unauthorized disclosures by a disgruntled employee. The key is to have a flexible response team with roles and responsibilities defined in advance.

Most security and privacy incidents go undetected. The third step in your proactive program is to **actively watch for trouble**. Monitor system audit logs. Make sure that patients and clients are aware of complaint procedures. Train staff to identify and report suspicious activity. Monitor alerts issued by government and security organizations such as CanCERT (Canadian Computer Emergency Response Team).

recollections are not. Record any information relevant to the incident such as phone calls, mail messages, and details of interviews with people directly involved with the incident. Track dates and times of anything. Ask people directly involved with the incident to write down exactly what they know about the situation.

Next, alert your incident response team, then **lock down and preserve evidence**. Isolate any physical or system resources that may contain evidence. This includes paper files, computer workstations, electronic records, email files, etc. Take any backup tapes out of circulation so that they aren't overwritten and backup any system resource associated with the incident.

If someone has been injured or aggrieved in any way, make sure that you **help the victim**. Acknowledge the victim's injury (without necessarily admitting any wrongdoing - not unless you are able to determine fault at this stage). Take whatever action is required to mitigate any negative circumstances. Keep the victim informed as appropriate about the progress of the investigation.

Quickly **determine the severity of the problem**, though this may be difficult at an early stage of the investigation. Determine if the issue needs to be escalated to senior management, if law enforcement agencies need to be notified, how quickly resources can be released back into production, and if there is a need for a contingency plan. It is important to have a measured response to the incident. We shouldn't make a capital case out of every incident. You don't send in the army to shovel snow (unless you're in Toronto).

As soon as possible after the incident, you need to **consolidate the evidence and get back to normal**. If law enforcement agencies are involved, they will determine when the yellow tape comes down. Otherwise it's a judgment call. You want to ensure that normal

operations resume ASAP while preserving evidence. Make sure that you image or duplicate paper and electronic records. Secure hard drives and other media storage devices. Replace them if necessary. Maintain vigilance. The attack may still be in progress or may be repeated.

While an incident or investigation is in progress, you need to tightly **control communications**. Designate someone to coordinate communications with the media and the victims. Restrict information concerning the incident to those with a need-to-know. Restrict the use of email and other forms of communications that can be monitored, such as cell phones. Keep communications short and factual. Avoid opinions or explosive rhetoric.

If an employee is involved in the incident, it may be necessary to invoke **disciplinary procedures**, such as short-term suspension, while the investigation is underway. In this case, management, HR and union officials must be kept in the loop as required. Other HR actions may take place as more information about the incident becomes known.

The investigation may continue long after the actual incident has occurred. The next stage is to **investigate the cause** and determine what longer term action may be required. You need to determine who had the opportunity to cause the incident. What was their motivation (e.g. hacker, malicious employee, or whistleblower)? Was this incident related to other incidents? Is this part of a pattern? What resources and methods were exploited and from where did it originate?

If an incident is found to be real (and some are not), it is necessary to **take appropriate action**. The most obvious is prosecuting the offender, either through legal proceedings, disciplinary or other HR action (e.g. training for someone who legitimately didn't know better). You need to implement corrective measures to ensure that the incident doesn't recur. And finally, you need to address the needs of any victims of the incident.

At the conclusion of the investigation and any subsequent legal or disciplinary proceedings, you should **document and learn**. A post-mortem with the incident response team will help the team to understand how and why the incident occurred. The team should also review its own handling of the incident and consider how effectively it managed the situation. Finally, it is useful to integrate any "lessons learned" into your security and privacy awareness program. Nothing makes a better "case study" than something that really happened.



What PRIVA-C means for you... and your clients.

New Legislation. New Concerns.

The result? Increased Accountability and Responsibility.

When it comes to privacy protection, we have the know-how and the tools — *a total solution*. And, we have the track record you can depend on. PRIVA-C's experienced consultants have helped health organizations deal with privacy issues for over a decade.

Let us help you navigate the pitfalls of privacy compliance. Build trust with your clients. Avoid risk.

A sound investment. Just ask our clients.

Offices located in Toronto and the Maritimes

Contact us at:

1-800-842-6077

info@carelink.ca

www.ehealthprivacy.com

PRIVA-C
A Division of CareLink