News

Protecting the scene of the crime

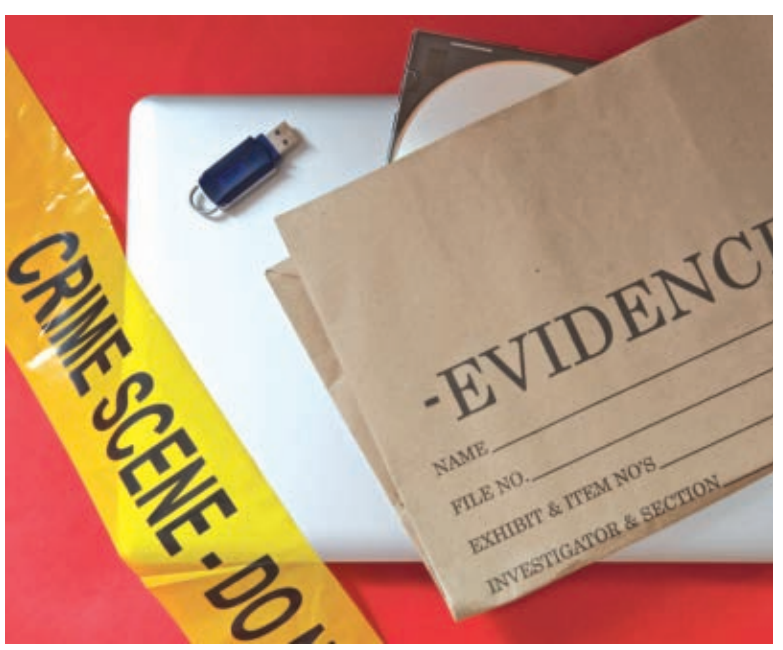
Preserving evidence is of the utmost importance after a cyberattack

JEFF BUCKSTEIN

Your company's computer has been hacked. As the first responder on the scene, your initial instinct could be to immediately shut down the system to prevent any more damage or intrusions. But that's exactly what you shouldn't do, experts say.

They warn that when it comes to cyber-incidents or suspected online crimes, shutting down systems right away might inadvertently hamper the forensics team's efforts to painstakingly piece together a picture of what happened.

"Preserving the evidence has to be the first priority. First responders need to make sure that it's handled appropriately in order to prevent destruction or compromise of the evidence," says Rob Frank, a partner with Norton Rose Fulbright in Toronto. "That's necessary in order to allow for a determination later on of how the breach occurred, and how the systems were compromised, and prosecution of the attackers where appropriate."



GRUMPY59 / ISTOCKPHOTO.COM

Even in the forensics world, the thinking until a few years ago was that the computer needed to be shut down right away. But that response changed when random access memory (RAM) started to get so large and important, says

CYBER SECURITY SPECIAL FEATURE

Kevin Ripa, the founder and owner of Computer Evidence Recovery in Calgary.

RAM contains a treasure-trove of information — passwords, chat logs, and a record of services and programs that were running while the computer was on — that doesn't exist anywhere else in the computer once it has been turned off, Ripa says.

"If you shut the computer off without collecting that, you potentially lose access to ever getting at that data on the hard drive. You lose access to any malicious software that had been running on the computer. It's called volatile memory and it disappears. So that's very, very important. If the computer is on, you must properly collect the RAM to image the hardware before you turn the computer off," he adds.

Even though certain steps should be followed before the computer is turned off, the reality is that by the time the first forensic responders arrive, depending on who else might have been on the scene before and what they have done, the computer might be either on or off.

If it's on, it needs to be kept isolated from the network, says Ripa. For example, with a desktop computer, the Ethernet cable can be unplugged to take it off the Internet. A laptop can have its wireless function turned off so that it can no longer be accessed by the Internet.

"If it's off, leave it off. Disconnect the power, and put the computer somewhere safe. Start a chain of custody on it, so that you can [account for] every minute, and get hold of a forensic specialist," says Ripa.

Experts say potential tensions could exist between first responders to a cyber-incident, based on the perceived need for

React, Page 27

Union: Concern is blanket ban stops prosecutors from running

Continued from page 1

the objectives of the PSEA.

Justice Kane agreed that the commission's denial of Taman's request did limit the ex-Crown's ss. 3 and 2(b) *Charter* rights to run for office, and to freedom of expression. However, she ruled the commission reasonably concluded that the incursion on Taman's *Charter* rights was outweighed by the need to ensure that the Office of the Director of Public Prosecutions (DPP) and its prosecutors are independent and politically impartial, and perceived by the public to be so in discharging their mandate, which includes prosecuting federal politicians and lobbyists.

"The decision reflects that the Commission considered all the facts and, based on its overall view, determined that the applicant's rights could not be fully protected while at the same time maintaining the objective of political impartiality in the public service," wrote Justice Kane, a senior criminal law policy official with the federal Department of Justice before joining the bench in 2012.

"The reality is that it is not always possible to strike a perfect balance either between competing *Charter* rights or between *Charter* rights and other rights and interests. Some rights may be required to give way to others in a manner which will be considered disproportionate by one party or the other."

The judge also held it reasonable for the commission to reject Taman's suggestions that instead of compelling her to choose between running for office or her job, the DPP could reduce the negative impact on her *Charter* rights by, for example, reassigning her to a non-prosecutorial position, or not assigning her politically sensitive files, when she returned to her post. The commission accepted the DPP's assertion that this was not feasible in an office where the main work is prosecutions.

Taman, the daughter of ex-Supreme Court Justice Louise Arbour and former Ontario Deputy Attorney General Larry Taman, lost to incumbent Mauril Belanger in the longtime Liberal stronghold of Ottawa-Vanier in the Oct. 19 election, receiving 12,299 votes to Belanger's 36,150.

> "We are disappointed with the result and, if we were to appeal, we would certainly bring to the Federal Court of Appeal's attention the broader implications of this case to prosecutors, and to all public servants.
>
> **Christopher Rootham**
> Nelligan O'Brien Payne

The Federal Court's judgment acknowledges that the DPP clearly opposes political involvement for PPSC prosecutors. Yet "the Commission's decision is not a prohibition against all federal prosecutors, as the decision was made based on consideration of the applicant's specific request and related to her specific duties," Justice Kane wrote. "Other requests would be determined on a case-by-case basis."

Taman's counsel, Christopher Rootham of Ottawa's Nelligan O'Brien Payne, said his client is considering an appeal. He told *The Lawyers Weekly* the rationale justifying why Taman was denied permission to run and take an unpaid leave of absence — to preserve the public's confidence in the DPP's independence and political neutrality — would seem to apply to all prosecutors.

"I think the only way to read it is [the judge] only left [the door] open a crack" to federal prosecutors being able to run for office, Rootham said. "We are disappointed with the result and, if we were to appeal, we would certainly bring to the Federal Court of Appeal's attention the broader implications of this case to prosecutors, and to all public servants."

Leonard MacKay, the federal Crown in Halifax who leads the Association of Justice Counsel which is supporting Taman's judicial review, said the union is concerned that a blanket ban on prosecutors running for office has effectively been created.

"The job description that was provided to the [commission] in relation to Ms. Taman…would describe virtually any prosecution job in Canada," MacKay said. "It wasn't specialized, or as high level, as the Federal Court might make it out to be. The description really is of any front-line prosecutor in Canada.

"The union's position is that the vast majority of prosecutors… should be allowed to run."

MacKay pointed out that many provinces permit at least some of their Crowns to run for office.

He argued the court also gave "short shrift" to Taman's argument that the PPSC could take measures to mitigate the impact on her *Charter* rights, such as erecting firewalls and not assigning her the relatively rare cases that are politically sensitive.

"I think they can accommodate that operationally, and they just decided not to because they feel strongly about this issue.

"If we are talking about balancing an individual's *Charter* rights versus the constitutional convention of impartiality and loyalty of civil servants, maybe it needs to go to a higher level."

The PPSC did not comment on the judgment.

Apart from her judicial review application, Taman is grieving what she maintains was her dismissal from the PPSC. Her former employer contends she abandoned her post by running for office after the commission denied her permission to do so.

News

React: Response team should be multitude of professionals

Continued from page 12

different approaches. For example, while the first priority of the information technology team is to frequently try and eliminate the source of the attack and staunch the bleeding, legal professionals have to look beyond an immediate fix.

"We frequently see the internal counsel being engaged right away in terms of response to the incident, thinking 'what are the preservation obligations that we have as soon as we learn about the incident?'" says Molly Reynolds, an associate with Torys LLP in Toronto whose practice focuses on privacy and e-discovery issues involving corporate, commercial litigation and class action suits.

The message needs to filter throughout the organization: Evidence cannot be changed or damaged in the process of resolving technological issues.

"Think about the potential for litigation down the road," says Sarah Graves, a partner with the labour and employment group of Fasken Martineau in Toronto. "Even if you have gathered evidence, think about issues like chain of custody, how you're going to prove what happened to the data, who gathered it, and how they gathered it. Because that evidence will have to come in at some point in legal proceeding."

Take a situation where a company's website has been hacked. Proper preservation can help demonstrate what was actually done, instead of having to rely on speculation or hypothetical explanations, if allegations arise in future litigation regarding how hackers accessed the website and how they were able to change information that was displayed, stresses Reynolds.

When you first become aware of a cyber-incident, a number of things need to be carefully monitored so that evidence is preserved without alteration, says Graves.

"You don't want to write over metadata. You don't want to destroy paths. You want to make sure you capture all the information on the servers, the desktops, the laptops, the handheld devices — on all of the sources of data that can be involved," she adds.

Another aspect concerns the appropriate response by your organization, which might differ somewhat from another company's procedures. Professional judgment is required to decide how best to contain the problem and preserve evidence.

The factors behind the decisions made along with any alternatives considered also need to be documented, says Reynolds.

ANDREYPOPOV / ISTOCKPHOTO.COM

> Preserving the evidence has to be the first priority. First responders need to make sure that it's handled appropriately in order to prevent destruction or compromise of the evidence.
>
> **Rob Frank**
> Norton Rose Fulbright

Multiple considerations can go into making that judgment call. They could be financial, taking into account the costs of certain preservation actions. They might be risk-related, such as a determination about whether moving information elsewhere could leave it vulnerable to attack. They could be technology-related — for example, if information is stored on a backup tape, you may need to consider whether future sources of technology will be able to access the data.

"Document those considerations that went into the decisions that were made, so that it shows the company was thinking right at the outset about responsible preservation," Reynolds says.

Another possibility arises if your system is suddenly shut down in the aftermath of a targeted attack that is based on a long period of undetected systems reconnaissance. It could immediately signal to the perpetrator that something is suspected, which can make the situation worse.

"If you try to stop it too soon, you're tipping the hand of the people who are doing this. They can start executing other stuff on the network that you didn't see, causing far more damage than would otherwise have been caused. So although stopping what's going on seems to be the right thing to do, it can actually be causing a lot more grief," says Ripa.

Many companies are potentially vulnerable to a cyber-attack, particularly those that collect sensitive customer data or that retain intellectual property or other confidential business information.

> We frequently see the internal counsel being engaged right away in terms of response to the incident, thinking 'what are the preservation obligations that we have as soon as we learn about the incident?'
>
> **Molly Reynolds**
> Torys LLP

The most common cyber-incident is known as a "phishing" attack, where somebody is fooled into clicking on a link and entering personal information from what they believe is a trusted authority, such as their bank, says Ripa.

If perpetrators are able to get that sensitive information, they can then use it as leverage to move around the network unfettered and with escalating privilege, causing untold harm by making unauthorized changes, exfiltrating data, and using the network to launch an attack on another network, he says.

"The planning really starts before you ever have an incident. Having procedures in place and a response team ready before you are ever the target of these types of issues is key, I think," says Graves.

Ripa agrees. "It's like any disaster response. [If] there's a fire in the building, you have all of that figured out before there is the fire. Because the No. 1 thing that is not on your side is time. The longer it takes you to respond, the worse that it is."

The response team should include a multitude of professionals from different groups including IT security personnel, in-house and/or external counsel, privacy officers, and possibly also human resources, customer service and public relations people, says Graves.

"Many organizations today are getting a full understanding of where they're vulnerable, and are then putting one of these teams in place so that when they have an incident they can move fast. They know who is responsible for what, who can decide what, and how to deal with the computer evidence in a way that is effective," she says.

Putting together such a team not only mobilizes your organization. It reduces the chances of conflict and increases the likelihood of reconciling the simultaneous needs to maintain the integrity of your system and preserve evidence in the aftermath of a cyber-incident.

"You have to have kind of an authority chain of who's permitted to take down systems and networks, who's going to collect the evidence. Set up your incidence response team with people who either have an ability to undertake the forensic analysis or understand the workings of it, so that you avoid destruction or compromise of the evidence," says Frank.

We want to hear from you!
Send us your verdict:
comments@lawyersweekly.ca