The General Counsel's Guide to Digital Defense_

THE LEGAL SIDE OF CYBERSECURITY

Contents_

About the cover_

Our cover utilizes a background of 1s and 0s, the language of binary, a system of numerical notation used internally by computers. GCs may not need to read binary, but even a familiarity with technology tools will aid cybersecurity, as detailed in this report.

Introduction_

If there is one universal truth about cybersecurity in today's business climate, it's that cybersecurity is everyone's problem, and everyone's responsibility.

Black Hat, a global information security event organization, brings together hundreds of top information security professionals every year for its US conference. In 2016, it surveyed its attendees to determine the top threats and concerns facing this community.

The results are startling, and clear: security pros overwhelmingly believe that their organization will likely face some type of security breach within the next year (72%), but even more importantly, a large majority also stated that they feel underprepared to deal with the impending threats. The most common reason cited for this was "a lack of qualified people and skills" (37%) followed by "a lack of commitment and support from top management" (22%). Only 31 percent of respondents felt that nonsecurity professionals in their organization fully understand the threats facing them today and support IT in combating those threats.

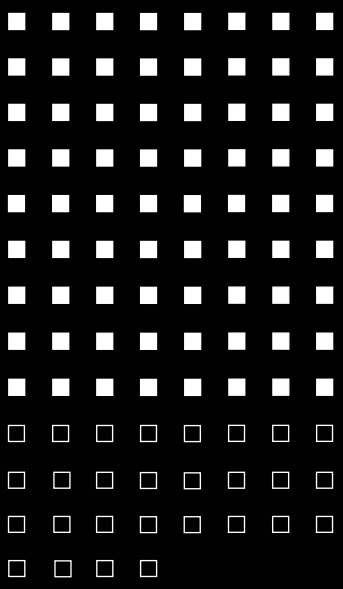
And the threats are increasingly aimed at targeting non-security professionals, who are more susceptible to phishing scams, social engineering attacks, and violating security policies. In fact, "end users who violate security policy and are too easily fooled by social engineering attacks" was identified as the weakest link in today's enterprise IT defenses by 28 percent of respondents, and 46 percent said that "phishing, social network exploits, or other forms of social engineering" were their greatest concerns.

IT professionals feel overburdened and understaffed, and they know they cannot act alone in protecting their organizations. They also know that even with the best prevention efforts and intentions, data and security breaches are increasingly likely.

According to a special report by information security company FireEye, law firms specifically are seeing a significant increase in cyber breaches involving advanced malware. The 2015 report states that in the legal sector, "common attack vectors are through e-mail and the web. Attacks […] typically tamper with users' web browsers and steal data, including legal strategies, and confidential information on clients and opponents. Attacks of this nature can complicate victims' cases and create additional legal problems."

72% of security pros believe their organization will face a breach within the year

1 ■ = 1%



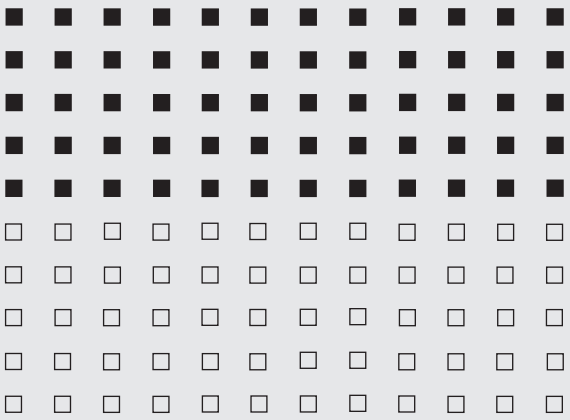
PREVENTION

Correcting for Human Error_

_ As these threats rise in frequency and intensity, it's imperative to recognize that each and every employee can be susceptible. Any individual who works with an organization using a company computer or phone can be a target of attack. Information security is such an important factor that it cannot solely be the focus of an IT department. Every individual must be ready to prevent these attacks, and the legal and IT teams need to be prepared to respond to a large number of potential scenarios if security is breached. The ROI is undeniable: a recent study from the Ponemon Institute found that cyber crimes cost the surveyed organizations on average $15 million per year.

According to Exponential Interactive general counsel Thomas Chow, keeping track of who has access to your files is essential. "A company's employees and contractors are its greatest cybersecurity risks. Disgruntled employees, improper access granted, theft of confidential data, information leaks, use of unknown USB flash drives—this is the stuff of nightmares for IT departments," Chow says. Luckily, these sorts of errors are preventable, by keeping careful control of access. Equally essential is knowing exactly what information and data the organization may have stored, and how it might be targeted. Even small companies can now gather and store massive amounts of data, and keeping abreast of what information you have will better prepare your legal, tech, and executive teams to deal with different types of attacks.

A study from the Ponemon Institute found that cyber crimes cost an organization, on average, $15 million per year.



PREVENTION

Cloudy With a Chance of Data Breach_

As legal professionals can now access confidential documents and data at any time from any device through cloud computing, the American Bar Association has made recommendations for keeping client confidences on web-based records. In addition to handling their clients' data safely, attorneys need to make sure their staff are following these same criteria to protect the confidentiality, integrity, and availability of this information. In fact, organizations in many states and industries are expected to follow reasonable data security measures. As examples, the Gramm-Leach-Billey Act details regulations for financial institutions, the health-care industry is bound by HIPAA security regulations, and states such as Texas, California, and Massachusetts require businesses that handle residents' personal information to protect that information.

According to Crista Harwood, senior vice president, general counsel, and chief administrative officer at Passport Health Communications, attorneys would be best served by being as familiar with the technical aspect of the security as the legal. "I would love to see more attorneys with technical backgrounds," she says. "It truly is a great combination. It gives me credibility when I'm talking about new technologies and when I'm discussing security concerns." As a prime example of this, Harwood details the encryption that all Passport patients go through, as well as the industry-leading fraud-protection programs it has in place. While she may not need the technical skills to code these developments, she needs to be aware of the HIPAA security regulations that would necessitate their adoption, as well as what exactly the programs do to fulfill patient expectations.

> **"I would love to see more attorneys with technical backgrounds. It truly is a great combination."**
>
> CHRISTA HARWOOD_
> SENIOR VICE PRESIDENT, GENERAL COUNSEL & CHIEF ADMINISTRATIVE OFFICER
> PASSPORT HEALTH COMMUNICATIONS

These regulations can cross over each other and create complex webs of security demands, so legal teams should be aware of what processes the company and their team will be expected to follow from this perspective. This web of regulations and laws becomes even more complex for any organization doing international business. Legal and industry guidelines vary from state to state, country to country, industry to industry, and the rules and the technology that these guidelines govern are in a constant state of flux.

Thomas Chow notes that preparation is important, but can only take you so far, considering the pace of technology. "It's nearly impossible to anticipate changes, so we've learned to scramble, quite effectively, to catch up with the issues that constantly blindside us," he says.

FINDINGS

A Global Threat_

The United States is the fourteenth-most-vulnerable country in the world in terms of server security, according to a 2016 article published in The Guardian. Below, nations are ranked by vulnerability, based on an Internet “heat map” showing servers with easy access for hackers.

1. Belgium
2. Tajikistan
3. Samoa
4. Australia
5. China
6. Hong Kong
7. Dominican Republic
8. Afghanistan
9. South Africa
10. Ethiopia
11. Kenya
12. Gabon
13. France
14. United States
15. Mozambique
16. Japan
17. Qatar
18. Yemen
19. Russian Federation
20. Argentina
21. Maldives
22. Azerbaijan
23. United Kingdom
24. Turkmenistan
25. Algeria
26. Korea, Republic of
27. Peru
28. Nigeria
29. Turkey
30. Hungary
31. Malaysia
32. Congo
33. Taiwan, Province of China
34. Czech Republic
35. Bahamas
36. Latvia
37. Ukraine
38. Slovenia
39. Austria
40. Croatia
41. Denmark
42. Luxembourg
43. Israel
44. Macedonia
45. Pakistan
46. Cyprus
47. Germany
48. Switzerland
49. Singapore
50. Vietnam

PREVENTION

Learn from the Tech Team_

_ A strong relationship with IT team members and the willingness to learn from them are extremely valuable. Communicating on a regular basis will ensure that the legal team won't miss out on any valuable information, and build the basis to allow legal to make better-informed recommendations. "If you haven't had lunch with the IT lead, do that," suggests Thomas Chow. "That will lead to understanding of IT systems and technology. If you don't have a general idea of your production environment server architecture, you really ought to."

Awareness of regulations and how they affect the company is one thing, but putting together a plan for the company to follow is another. A data breach can be as simple as an under-educated employee sending confidential data via personal e-mail, and education can just as simply cover these gaps. To this end, employee training and education are essential steps. This can start with making sure that all members of a board are aware of how important this adherence to cybersecurity can be.

For any organization, two key elements of prevention are employee training and cutting-edge technologies. For general counsel, the former may seem to be more in their purview than identifying and applying high-tech solutions. That said, attorneys make technology choices on a daily basis, even ones as simple as which app to use to convert a file or what e-mail server to use. The Global Privacy Enforcement Network issued an annual privacy sweep of mobile apps in 2014, and found that 59 percent of apps inspected failed to provide sufficient information regarding user privacy prior to installation, and worse, 31 percent sought excessive permissions—meaning that these apps gave the provider too much access to the user's device and network. Downloading any of these apps on a personal phone that an attorney also uses to conduct business could be just as damaging as a malicious attack from an outside source.

In fact, a 2016 study by the Ponemon Institute found that, on average, the data contained within an individual's mobile device would be worth $14,000. Further, if this is true of the average individual, a cyber attacker's ability to access the files of many individuals located on the personal device of a single legal professional makes this sort of attack a potential bonanza for the criminal. For that reason, legal professionals need to be aware that they are viable targets for hackers as well as potential serious problems to their clients if they're not sufficiently educated themselves.

> 59% of apps inspected failed to provide sufficient information regarding user privacy

Finally, one thing many companies consider part of a breach readiness plan is cyber liability insurance. This coverage can be an important part of preparation for a breach, potentially covering response costs like hiring security forensics experts, public relations costs, identity theft resolution services, data restoration, and more.

RESPONSE

Death, Taxes & Data Breaches_

_ Few things in life are guaranteed, and unfortunately your organization becoming a victim of a successful cyber attack could be considered one of them. No matter how rigorous the prevention plan, defense can never be enough when cyber criminals get more sophisticated by the second. Terry Kurzynski, a senior partner at HALOCK Security Labs, tells clients that it's better to think about when, not if, a cyber incident occurs. Prevention is critical, but so is preparation for the inevitable.

"The industry needs to invest more in incident response capabilities versus only on protection investments," Kurzynski says. "The goal is to reduce the compromise-to-remediation time frame from a couple hundred days to a couple hours or less."

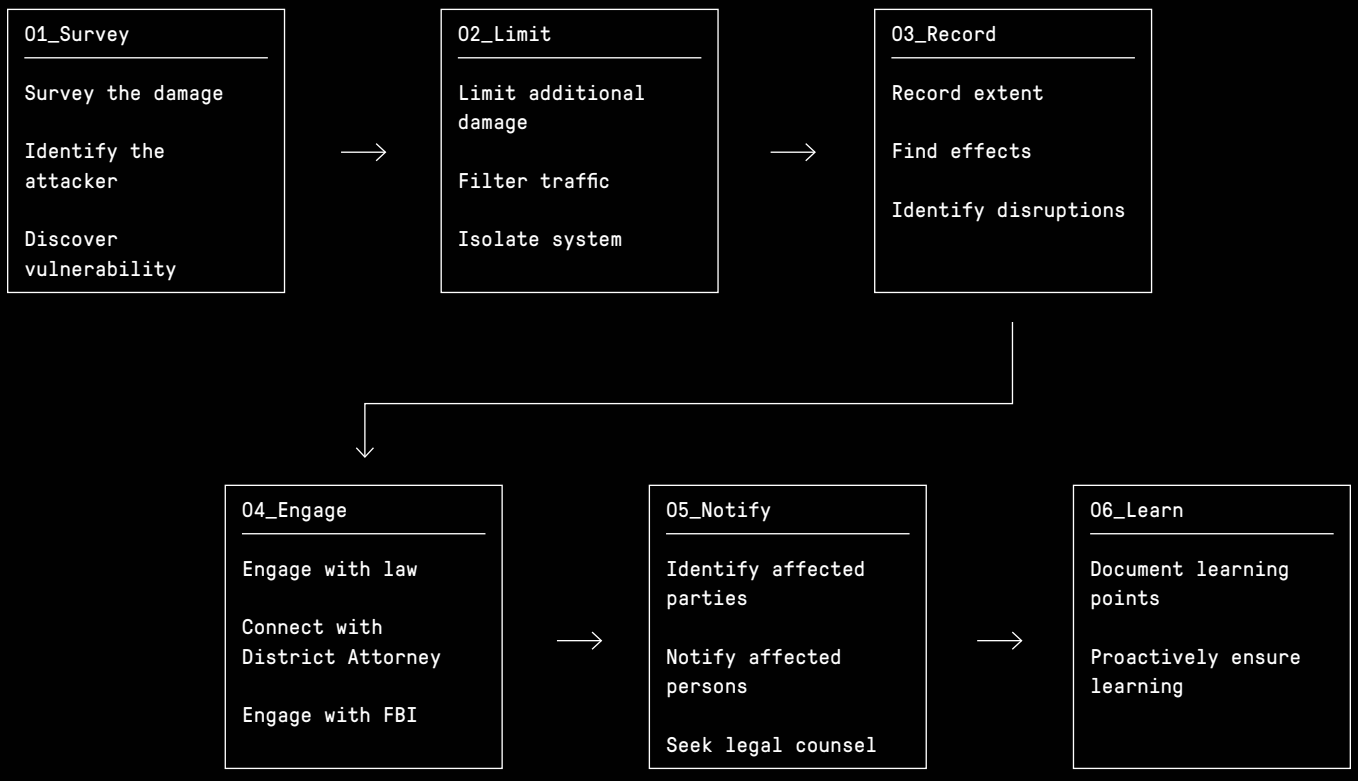
From the legal perspective, that means thinking about how your organization will handle issues like informing customers or vendors about data breaches, and making sure that all communication about the incident goes through attorneys and is thus covered by attorney-client privilege.

> **"The industry needs to invest more in incident response capabilities versus only on protection investments."**
>
> TERRY KURZYNSKI_
> SENIOR PARTNER
> HALOCK SECURITY LABS

Examples of poor handling of data breaches have led to highly public lawsuits and PR nightmares, so thinking about the legal elements of how and when an incident should be disclosed is crucial for in-house attorneys. Kurzynski also points out that having a detailed incident response plan in place can help show judges that a duty of care was met, and limit your organization's liability in the event of the loss or compromising of sensitive customer data. "Judges are not in a position to determine whether a particular control is adequate or not," Kurzynski says. "What they do understand is whether or not you've demonstrated your duty of care. What actions did you take to treat those foreseeable risks? Has the organization performed activities to foresee and reasonably address its risks?"

FINDINGS

How to Respond to a Breach_



RESPONSE

All Hands on Deck: Creating an Incident-Response Plan_

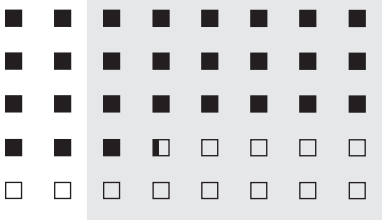
_ One of the requirements of operating in a world full of cyber risk is the ability to prepare for multiple scenarios. The proposed US Cybersecurity Disclosure Act of 2015, if passed by Congress, will require publicly traded companies to disclose in their annual reports whether any member of its governing body has cybersecurity expertise. Failing that, it will require the company to explain what steps are being taken to bring such an individual into the company's governing body. Regulators see cyber risk as a priority, and so should you.

A large part of the legal department's responsibility in the cybersecurity realm is in translating compliance and legal issues into actionable steps that IT can take, both before and after a breach. In-house attorneys also can keep senior leadership across departments informed about what they can each do to address these risks. Pam Krop, the general counsel of RevGroup and formerly of Intermedix, says that legal departments need to spend as much time working together with IT as they do with finance and HR. Take, for example, the "US State of Cybercrime Survey," conducted by PwC in 2015, which found that companies without training lost an average of $683,000 per security incident.

Jonathan Matkowsky, president of Matkowsky Law and Maccabim.com, an online brand threat mitigation platform for IP counsel and business executives, advocates for companies to adopt cross-functional teams or steering committees that actively work on not only cyber threat detection and prevention, but also response. But if that's not possible, assuming that your company has its cyber threat response plan in place and ready from an IT perspective, what can the legal team do to catch up?

"Assess it and make sure there are policies and procedures in place to implement the plan," says Matkowsky. "Make sure it complies with statutory and regulatory requirements, in addition of course to any contractual commitments, company policies, and external communications, as well as industry best practices. Then audit the plan from time to time to ensure that it is being updated as the company and/or as requirements evolve." Beyond having an incident-response team that includes all relevant company stakeholders—including legal—it's important to make sure your plan works through simulation and auditing.

$683,000: The amount that companies without training lose on average per security incident



RESPONSE

Know Your Rights—and Someone Who Knows Them Better_

When it comes to disclosure, complete and immediate notification is not always best. "You want to make sure you are providing accurate info to your customers and the public," explains Chad Layton, a shareholder of Segal McCambridge Singer & Mahoney who regularly represents clients following cybersecurity incidents. "You don't want to make the mistake of disclosing too early because your information may not be accurate, and you don't want it to be confusing." Part of your preparation may be retaining outside counsel that specializes in how to respond to cybersecurity breaches; that retainer may also constitute part of your response plan that proves your organization is taking threats seriously.

Another area to consider when thinking about limiting liability is in vendor security. "If you're a company that shares data with other vendors, make sure they have cyber insurance—and that you have the right to audit them to make sure they are properly protecting any data that might be shared," says Layton.

Auditing may fall to an internal audit team, but it's also recommended to outsource particular audits. These include SOC 1/SSAE16, to test key business and technical controls by a licensed accounting firm; PCI tests for businesses that transmit or process credit card data; ISO tests for international security standards; and penetration tests to determine particular network weak spots.

> **"The public has the perception that you can make yourself impervious to attack, but that simply isn't possible."**
>
> PAM KROP_
> GENERAL COUNSEL
> REVGROUP

"No matter what you do, there will be vulnerabilities in security," Pam Krop says. "The public has the perception that you can make yourself impervious to attack, but that simply isn't possible. I can tell you from experience that going through reporting and notification is excruciating. [...] But acknowledging that a breach has happened is essential so that everyone can share experiences and use them to develop better protective measures."

And while having a dedicated team across departments can help you keep up to date on the latest breach protocols, you should never assume you know enough. Matkowsky, the former legal director for Yahoo's brand protection team, identifies the most important step that a general counsel must take after a breach: "Make sure that the breach notification plan is being implemented, but supplement as needed with expert outside counsel," he says.

FINDINGS

Prepare a Response Plan_

Your cybersecurity policy must include directions for preparing a response plan. Your response plans should answer the following questions.

01_Who will be notified?

All clients?

Only clients whose information may have been accessed?

Only clients whose information you confirm has been accessed or stolen?

02_What is your notification timeframe?

Do you rely on the maximum time allowed by law (30 or 60 days in most cases)?

Do you decide on a case-by-case basis?

03_What documentation must be kept regarding the breach?

The minimum required by law?

The minimum necessary to present to an ethics committee?

04_Who is authorized to speak about the breach?

To clients?

To law enforcement?

To the press?

05_Who is authorized to make critical decisions?

About the investigation?

About retaining documents?

To authorize the IT manager to proceed through steps to restore systems?

RESPONSE

Document and Comply_

When an incident is discovered, take the time to determine the scope of the attack. Once that has been completed, it's important to take detailed records in order to assist law enforcement and any third-party security experts kept on retainer. While the legal team does not have to be directly responsible, it should have some oversight into what data needs to be logged and retained to best position itself if litigation ensues. Having a single employee retain all these records will help ensure proper handling and mitigate suspicion that evidence has been tampered with or altered.

The US Department of Justice recommends that the following information be retained:

- A description of all incident-related events, including dates and times
- Information about incident-related phone calls, e-mails, and other contacts
- The identity of persons working on tasks related to the intrusion, including a description
- The amount of time spent, and the approximate hourly rate for those persons' work
- Identity of the systems, accounts, services, data, and networks affected by the incident and a description of how these network components were affected
- Information relating to the amount and type of damage inflicted by the incident
- Information regarding network topology
- The type and version of software being run on the network
- Any peculiarities in the organization's network architecture, such as proprietary hardware or software.

RESPONSE

Recovering Ground_

_ Once the threat has been mitigated, it's important to know your organization's rights as a victim of cyber crime. Do your company's insurance policies cover cyber incidents? Do you know what your organizations liabilities are, and are you prepared for any litigation that may occur? Also, knowledge of the US Computer Fraud and Abuse Act is critical as it outlines what actions private companies and individuals can take in order to recover damages. (Again, the importance of being in lockstep with your organization's cybersecurity team is highlighted here as you may not be able to take advantage of your organization's cyber crime rights if you're unaware of an incident.)

The act contains provisions that not only outline assistance for recovering financial damages, but also assist in retrieving stolen data, such as stipulating injunction relief for former employees with improper access to your systems and data. For in-house counsel, it's important to identify any resources that can help defend against any harmful claims.

According to Thomas Chow, you might not be able to unring the bell, but you can make it more difficult for criminals to use stolen information. "Litigation with injunctive relief is appropriate, particularly when you have the forensic evidence to show there was actual theft of trade secrets," he says. "A TRO or preliminary injunction is almost always appropriate. At that point, it's really about litigation against the offending parties."

> **"Litigation with injunctive relief is appropriate, particularly when you have the forensic evidence to show there was actual theft of trade secrets."**
>
> THOMAS CHOW_
> GENERAL COUNSEL, CHIEF COMPLIANCE OFFICER & SECRETARY
> EXPONENTIAL

Conclusion_

Trends and data clearly show that the risk of a cyber breach is high for any type of organization. While the bulk of the responsibility for preventing and responding to these incidents may lie with the IT department or under the CIO's purview, the legal consequences will undoubtedly land on the desk of the GC. With that in mind, it's important to make cybersecurity a priority not just in your legal department, but throughout an entire organization.

The first line of defense has been proven to be awareness and education of all employees. Training in best practices to avoid breaches could be spearheaded by the legal team. Documenting this training could also help to prove a duty of care in the event of litigation stemming from a cybersecurity issue.

Another important part of preparation is simply knowing how your technology or IT department is structured, who is responsible for cybersecurity, and who you should be communicating with about the legal impacts of decisions the IT staff makes. Earning the team's trust is also important, so that when a breach occurs, they can notify the legal department and see legal as a true partner, not just an oversight arm.

Finally, developing and enacting a response plan is vital. Ensuring that every single employee understands their role and responsibility in responding to a cyber attack makes it much easier to deal with when it occurs. For the legal team, that means knowing who to talk to, what to document, and what data is the most sensitive. It also means being able to understand the extent of the breach so that it's clear what needs to be disclosed to law enforcement, board members, senior leadership, shareholders, or the public, from a public relations as well as a legal standpoint.

If the legal team sees cybersecurity as an important part of its work, that viewpoint will filter down to every department that interacts with legal, and will ultimately better prepare your organization to respond to an attack. Eleanor Lacey, the general counsel of SurveyMonkey, puts this into practice daily. "I give security priority over almost every other initiative," she says. "Implementation must be as fast as is reasonable for the company based on the type of data being protected." Lacey also emphasizes the importance of legal working side-by-side with tech ops and sharing information between departments so that both are fully equipped to handle threats and challenges.

> **"I give security priority over almost every other initiative."**
>
> ELEANOR LACEY_
> GENERAL COUNSEL
> SURVEYMONKEY

Attribution_

Guerrero Howe Custom Media

825 W Chicago Ave
Chicago, IL 60642

Phone: (312) 447-2370
Email: info@guerrerohowe.com
guerrerohowe.com

Editorial:
Megan Bungeroth
Jennifer Draper
Adam Kivel
Christopher James Palofox

Design:
Greer Mosher

Communications:
Kathleen Fox
Megan Wolter

Consultant:
Thomas Chow

Sources:

Black Hat Attendee Survey, 2016.

Bungeroth, Megan. “Crossing Your Fingers Isn’t a Cybersecurity Plan.” Sync magazine. Guerrero Howe, n.d. Web. 16 Sept. 2016.

Dhillon, Gurpreet, Ph.D. The Changing Faces of Cybersecurity Governance, What to Do Before and After a Security Breach. Rep. Richmond, VA: n.p., n.d. Print.

Focht, Brian. 12 Steps to Cybersecurity: A Guide for Law Firms. Rep. N.p.: CLIO, n.d. Print.

Hern, Alex. “Belgium Tops List of Nations Most Vulnerable to Hacking.” The Guardian. Guardian Newsand Media, 8 June 2016. Web. 16 Sept. 2016.

US Department of Justice. Computer Crime & Intellectual Property. Best Practices for Victim Response and Reporting of Cyber Incidents. 1.0 ed. [Washington, D.C.]: n.p., April 2015.