How IT Folks Can Protect Their Job Pre Breach

By Ray Hutchins and Mitch Tanenbaum

January 12, 2023

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

In September 2022, the Suffolk County government in New York suffered a ransomware attack that shut down county and municipal services and has cost over $5M…so far.

An investigation performed by Palo Alto Networks revealed poor IT management, a series of technical blunders, delayed security upgrades, unsuitable management structures and "obstructive behavior" from an IT director who was initially suspended but then fired. The fired IT director does not deny culpability, but says he warned county officials repeatedly of the vulnerabilities and was ignored.

We understand that the IT director will be suing the county. Perhaps more dirty laundry coming out on this…stay tuned.

A Wall Street Journal article about this situation can be found here: https://www.wsj.com/articles/suffolk-county-n-y-leaders-blame-clerks-office-for-cyberattack-11671673082

In October, Uber's former Chief Information Security Officer was convicted of criminal charges for his part in dealing with the 2016 Uber breach.

This is the future. IT and business managers will be called to account for what happened on their watch. So, whether you are in IT, manage IT or are a more senior manager, there are steps to take now.

In reality, the Suffolk County IT Director may be culpable, but so is county leadership. But who got the blame? The IT Director…and NOT the county officials. In the Uber case, it is a senior manager whose career is trashed and will likely be going to prison.

This type of situation will repeat itself again and again in the future. So how do IT directors, IT staff and other managers cover their butts and reputations in similar situations?

Here are some thoughts:

1. Make sure all your cybersecurity and privacy responsibilities are clearly defined and described in your work contract.or job description.
2. Make sure that any responsibilities assigned to you are correctly funded and supported by top management. In the case of the public sector, that means both your administrative supervisor and your political bosses.
3. Make sure that whomever you are supposed to report to with respect to these responsibilities is clearly defined in your agreement documents.
4. Meticulously perform your job responsibilities and DOCUMENT your activities with respect to your cybersecurity and privacy responsibilities.
5. Identify and document any managerial weaknesses with respect to organizational management ofcybersecurity and privacy risks.
6. Carefully document any organizational vulnerabilities.
7. Save copies of everything. Funny how when there's a problem, emails and other digital documentation starts to disappear. Paper copies are a good idea.
8. Make sure you're covered by the company's directors and officers liability policy. If they don't have D&O then ask them to do so and document that.
9. Also, you can consider using the whistleblower law. Whistleblower law rules are different in every state and you can't just blab at random and still be protected. That may require advice from a lawyer. Not one who is paid for by the company. That will determine whether or not you leak certain information, who you are legally allowed to leak it to and what protections you have.
10. If an incident occurs, inform everyone immediately and save all documentation.
11. Request time at all major organizational management meetings so you can present risk management issues to the right people. Make sure that you explain risk as a risk to the business and not some abstract technical risk.
12. Ensure that regular reviews of your performance are conducted and that your risk managementactivities are reviewed and approved. If there are any shortcomings identified, aggressively mitigate them and document your work and get that acknowledged and approved.
13. Your posture regarding risk management, cybersecurity, and privacy should be recognized by all stakeholders as an evangelist for doing better…and sooner. And for protecting the company's brand.
14. Build relationships with and work closely with any compliance officers.
15. Build relationships with your peers at other organizations in your industry to learn what they are doing successfully…and not so successfully and share what you learn with coworkers and management.

What about the flipside? How can management avoid this type of problem?

While the above applies equally to management and IT staff, there are some things that only management can do, including:

1. Assume full responsibility for cybersecurity
2. Implement a professional cybersecurity program based on a compliance framework
3. Correctly fund and staff the effort to build your program
4. Listen to IT staff concerns
5. Document all issues brought to you by IT and others and management's response

Want to discuss further? CyberCecurity LLC is a full-service cybersecurity and privacy firm that can help you meet your cybersecurity and privacy responsibilities.

Please email us at: mitch@cybercecurity.com

Did you find this position paper of value? Here are some of our other papers.

1. IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
2. GLBA & FTC Safeguards Rule
3. CMMC Compliance-The New Enclave Approach
4. The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis

About the Authors

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/