Clearwater

Whitepaper

Ransomware: The Need For a Business Impact Analysis

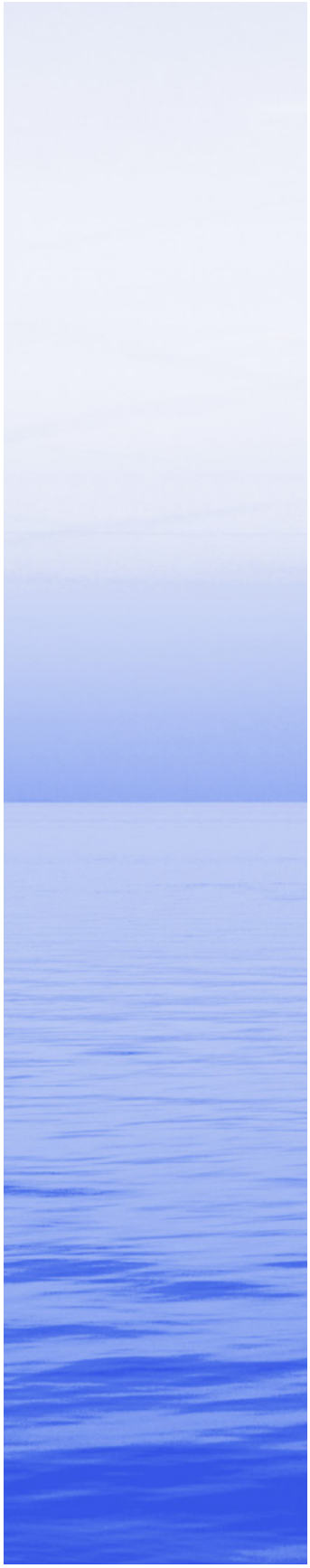
Cathie Brown of Clearwater on How to Improve Decision-Making in a Crisis

Introduction

Brown brings more than 30 years of experience in healthcare, health information technology, health information security and consulting to her work as Vice President of Consulting Services for Clearwater. In that role, she helps lead Clearwater's team of healthcare cybersecurity and compliance experts that assist healthcare organizations with developing and implementing effective HIPAA compliance and cyber risk management programs.

Over the course of her career, Brown has helped healthcare organizations mature across the HIMSS Analytics Maturity Models as a HIMSS Analytics Certified Consultant. Her experience also includes serving as Deputy Chief Information Security Officer for the Commonwealth of Virginia from 2006-2009 and 19 years with Centra Health, where she served as the health system's first Information Security Officer.

Brown is the incoming President for the Virginia HIMSS chapter, and she maintains certifications in security (CISSP, CISM), IT Governance (CGEIT), and Project Management (PMP).



You see the news: how many healthcare entities are struck by ransomware. But how many of them conducted business impact analyses before they were victims? Too few, says Cathie Brown of Clearwater. She discusses the value of doing a BIA before the crisis strikes.

"It is a troubling time for healthcare, particularly with ransomware," says, Brown, VP of consulting services. "I heard a report yesterday that there is an estimated ransomware attack every eight minutes. Healthcare is the top target [and] has been for a while now." Brown says the BIA not only will help dictate ransomware response, but it will assist in any type of crisis decision-making.

In an interview with ISMG, Brown discusses:

- Troubling ransomware trends;
- The value of conducting a BIA specifically for ransomware;
- How to operationalize the learnings from a BIA.

TOM FIELD: Hi, there. I'm Tom Field. I'm Senior Vice President of Editorial with Information Security Media Group. My topic today is ransomware and the need for a business impact analysis. Here to discuss this with me is Cathie Brown. She's Vice President Consulting Services with Clearwater Compliance. Cathie, thanks so much for taking time to speak with me today.

CATHIE BROWN: Thank you, Tom

FIELD: Oh, Cathie, I've got a big opening question for you. What are the troubling trends that you're seeing now with healthcare entities and ransomware?

BROWN: It is a troubling time for healthcare, particularly with ransomware. I heard a report yesterday that there is an estimated ransomware tech every eight minutes. Healthcare is the top target. It has been for a while now. But the hackers are really changing their approach. They're much more sophisticated. Their demands are much higher now. So for healthcare, I think the really troubling piece of this is, an attack on our healthcare industry is ultimately attack on patient care, and that's what bothers me most of all.

FIELD: So we see these attacks every week now. Of the ones that you've come in contact with, how many of these entities had done a business impact analysis before? Not after. Before they were [inaudible 00:01:30].

BROWN: Yeah, that's a really good question, Tom. Because I am a big believer in a business impact analysis. And a lot of the entities that I go into, that's one of the first questions I'll ask them. Because I do risk management work.

And I will have companies or healthcare, hospitals, whatever, tell me we do have a business impact analysis, but it's from 2004 and we haven't kept it updated. Business continuity and disaster recovery is absolutely a best practice. It's a requirement for risk management. And it's gaining a lot more attention than it has in the past, previously, because of current events. But I think that that critical business impact analysis step gets overlooked.

FIELD: Well, let's talk about that. What is the value of conducting a business impact analysis for a ransomware, or really for any other similar cyber incident?

BROWN: Sure. So the business impact analysis, what this really does is, it brings business to the IT table. So it brings the business into IT operations. The reason I say that this is a foundational component for risk management is because part of the business impact analysis is identifying what the critical processes are. Not the critical systems, but the critical business processes.

And from that, then we capture what systems are used. So from an IT perspective and also from a business continuity perspective, you're able to really plan around what the business needs. Rather than what IT believes to be true, which is what happens a lot. And having some experience with that, I know.

FIELD: Cathie, what are the critical components of business impact analysis? And which ones do you find are most often overlooked, or misunderstood, or as you say, taken in another direction altogether?

BROWN: Sure. So I think the critical components of the business impact analysis are really defining what those critical processes are for the departments across the organization. And it can be something like patient charting, OR supplies, payroll. These are critical functions that are just assumed to be there.

When they don't have the systems now, that has both a quantitative and a qualitative impact. So, what we're able to do with the business impact analysis is to define what those functions are. We have a formula that measures the impact, and then we can prioritize those processes. And by prioritizing those processes, we're able to prioritize the systems.

So, the priorities around the processes really go into a business continuity plan. The priorities around the systems go into a disaster recovery plan. And so that's really the basis. So you really develop your plans around your most impactful and most important business areas. Does that make sense? Hopefully.

FIELD: It does. But Cathie, beyond the immediate impact, how does the business impact analysis inform crisis decision making?

BROWN: Yes. So, in the case of a ransomware attack, I recently worked with a company that had a ransomware attack and I talked to their CIO. And they told me, I have no idea where their data is. Because when you have a ransomware attack, everything to everybody is all important. And so you don't really have a good way to prioritize how you approach the attack.

BROWN: So you've got everybody coming at you asking for all of their things. When you have a business impact analysis, you have a document that says patient access. What is it? I know you said you use these systems. You have a roadmap basically to respond to the incident or the attack. Again, that addresses the needs of the business.

FIELD: I want to bring this back to Clearwater Compliance. How does Clearwater Compliance help healthcare entities with their business impact analysis, either pre- or post-crisis? Hopefully pre.

BROWN: Yes, hopefully pre. We do help hospitals and our customers with business impact analysis. And we do that as a precursor to helping them with their business continuity and disaster recovery plans. Once you have your business impact analysis and your continuity and disaster recovery plans, then we can do a tabletop exercise with them.

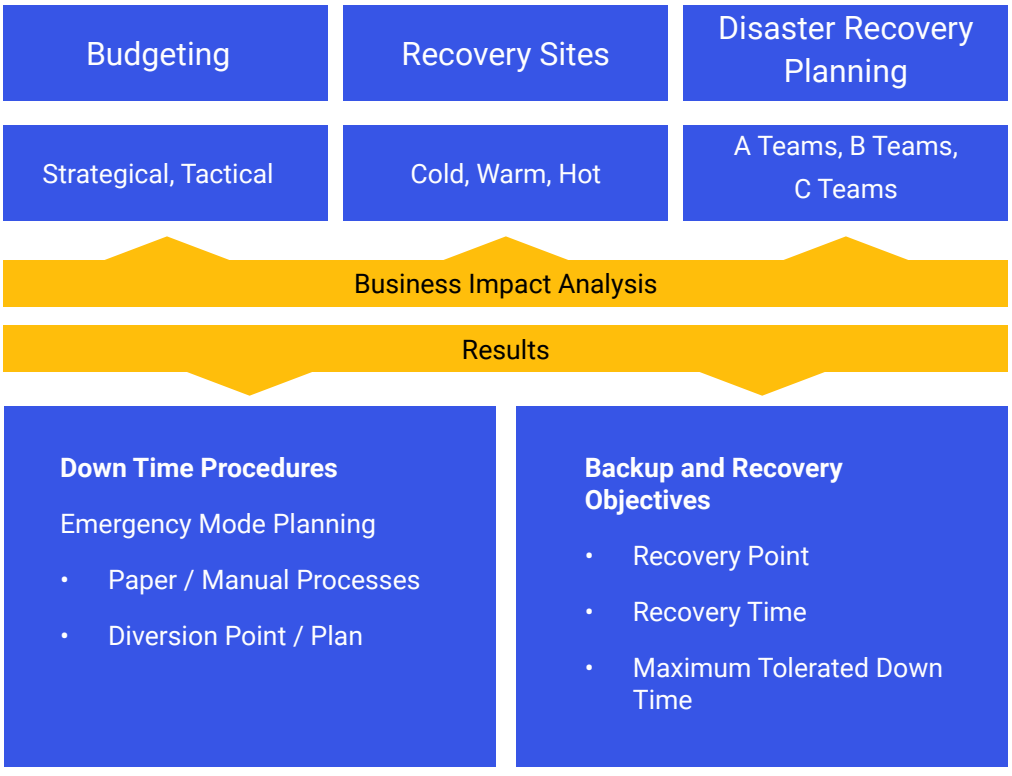
And we can simulate a ransomware attack. And what that provides for them, again, is a roadmap for how to respond. So the business impact analysis pre-attack, in my opinion, is critical to the response post-attacked. We can help them with pretty much evaluating what their response was and tying that back to the business.

FIELD: Well done. Cathie, I appreciate your time and insight today. Thanks so much.

BROWN: Thank you, Tom. I appreciate the opportunity.

FIELD: Again, we've been talking about ransomware and the need for a business impact analysis. You've just heard from Cathie Brown. She's Vice President Consulting Services with Clearwater Compliance.

For Information Security Media Group, I'm Tom Field. Thank you so much for listening today.



Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact