Deloitte.

THE RIPPLE EFFECT

Stories of purpose and lasting impact

Preparedness can flip the script on cybersecurity events.

A media and entertainment company's cybersecurity incident response plan needed a dramatic rewrite.

SUSPENSE BELONGS ON SCREEN, NOT IN AN INCIDENT RESPONSE PLAN.

THE SITUATION

Our story begins with a spoiler: A media and entertainment company was going to experience a cybersecurity incident.

Would it be an insider event originating within the company? A ransomware attack affecting operations? Or a breach of data from one of its many productions filming across the globe? The company couldn't predict how an incident would happen, or when … but it had to be prepared.

Even without an imminent, identifiable security threat, the company's chief information security officer (CISO) understood how—across industries—incidents can emerge at any time, from any place. He wanted to ensure his team is ready as potential threats evolve over time.

The company had gone through its own evolution and was growing its infrastructure, but its security posture hadn't kept up. The CISO had an ambitious vision that included driving efficiencies through automation. But before the company could explore new technologies, it needed to ensure the foundation of its cybersecurity incident response plan was strong.

The aggressive actions the CISO believed necessary for building resilience against threats ranging from low-level phishing to significant ransomware attacks would require participation and investment from all levels of the company. He could see where he wanted the program to go, and he needed to feel confident that when crises occurred, executive stakeholders would be able to act quickly to deliver a coordinated, rapid response to reduce risk and enable a sharper focus on actions that would have the most impact.

THE SOLVE

That was something our team of Deloitte professionals understood keenly. The engagement was led—coincidentally—by several former Air Force officers whose approach to protecting the media and entertainment company's intellectual property was driven not just by years spent helping clients defend against cyberthreats but also their experience protecting our national security.

We helped build out an effective incident response plan that leveraged people, processes, and technology. It was intended to change the perception within the client's company that responsibility for cybersecurity rested only on the CISO and his department, expanding it to bring a whole-of-business response since incidents can have an impact on the entire business. We worked closely with the CISO to help identify key stakeholders across the company and align them around the enhanced plan. We studied policies and processes already in place and helped adjust accordingly. We also looked at existing technology the company was using to detect cybersecurity events and how it could be adapted to isolate and contain them. Then we helped create a detailed playbook that would serve as a road map all stakeholders could follow.

The project culminated in a conference room, where we gathered leaders from not only security and IT, but from human resources, legal, finance, corporate communications, public relations, and more—the first time this group came together in a cybersecurity context—for an intensive exercise designed to replicate a real-world cybersecurity event. They meticulously followed the procedures an actual incident would require, enabling us to fine-tune the overall process and help these key stakeholders develop the response muscles they'd need when incidents occur.

PRACTICE ISN'T ABOUT PERFECTION.
IT'S ABOUT PREPARATION.

THE IMPACT

Back to the prologue: A few months later, that cybersecurity threat materialized.

It had the potential to have a negative impact on the company's employees, investors, and customer base. But because they'd exercised their collective response muscles, each corporate function understood what steps it needed to take, and the client successfully countered the threat using the whole-of-business response we helped them engineer.

The company's readiness derived from practice and a better understanding that cybersecurity incidents often raise cross-functional concerns, resulting in cross-functional responsibility. It's not a spoiler to acknowledge that additional events are likely to occur. But now our client has an actionable plan with demonstrated effectiveness and a team prepared to implement it together.

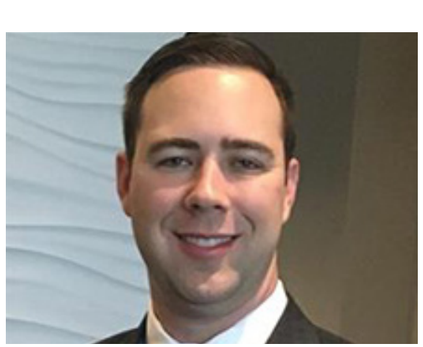
LET'S CONNECT.

Do these challenges sound familiar?

GLENN AGA
Managing Director
Deloitte & Touche LLP
glennaga@deloitte.com
+1 714 913 1070

KEVIN URBANOWICZ
Managing Director
Deloitte & Touche LLP
kurbanowicz@deloitte.com
+1 713 982 2309

JONATHAN GOLDSBERRY
Senior Manager
Deloitte & Touche, LLP
jgoldsberry@deloitte.com
+1 763 273 7646



BRANDON ROBERTS
Manager
Deloitte & Touche LLP
braroberts@deloitte.com
+1 713 982 3727

Deloitte.