

FLIPPING THE SCRIPT

(based on a true story)

IN THIS GRAPHIC ADAPTATION, WE BRING TO LIFE A REAL CASE STUDY ABOUT A COMPANY THAT ENGAGED DELOITTE TO HELP THEM CREATE AN INCIDENT RESPONSE PLAN IN THE EVENT OF A CYBERSECURITY ISSUE. THOUGH WHAT HAPPENS HERE IS A DRAMATIZATION, THE STORY IT'S BASED ON IS TRUE; THE THREATS OUT THERE ARE ENTIRELY REAL; AND ANY BUSINESS, IN ANY INDUSTRY, COULD FIND THEMSELVES IN A SIMILAR SITUATION. READ ON...

OUR STORY BEGINS WITH A SPOILER: A MEDIA AND ENTERTAINMENT COMPANY IS GOING TO EXPERIENCE A CYBERSECURITY INCIDENT.



1) CHIEF INFORMATION SECURITY OFFICER (CISO):

- RESPONSIBLE FOR CYBERSECURITY STRATEGY AND IMPLEMENTATION.
- ENSURES PREPAREDNESS FOR POTENTIAL CYBER THREATS.



2) INCIDENT RESPONSE TEAM:

- TASKED WITH RESPONDING TO CYBERSECURITY INCIDENTS.
- INCLUDES ROLES LIKE INCIDENT MANAGER, IT SPECIALISTS, AND CORPORATE OFFICERS (LEGAL, HR, PUBLIC RELATIONS).



3) BOARD OF DIRECTORS:

- RESPONSIBLE FOR ELEVATING CYBERSECURITY ISSUES ACROSS THE ORGANIZATION.
- ALLOCATES RESOURCES AND SUPPORTS THE CYBERSECURITY STRATEGY.



4) EMPLOYEES:

- NEED TO UNDERSTAND THEY ALL PLAY A ROLE IN CYBERSECURITY AND PARTICIPATE IN TRAINING AND SIMULATIONS.



5) DELOITTE PRACTITIONERS:

- CYBERSECURITY PROFESSIONALS PROVIDING ADVISORY SERVICES TO THE ORGANIZATION AND HELPING BUILD THEIR CYBERSECURITY INCIDENT RESPONSE PLAN (CSIRP).
- ASSIST IN DEVELOPING AND IMPLEMENTING CYBERSECURITY STRATEGIES, CONDUCTING RISK ASSESSMENTS, AND LEADING INCIDENT RESPONSE EFFORTS.



6) EXTERNAL PARTIES:

- INDUSTRY PEERS, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS THAT COLLABORATE AND SHARE INFORMATION ON CYBERSECURITY THREATS AND LEADING PRACTICES.

SOMETIME BEFORE THE INCIDENT...

LADIES AND GENTLEMEN, CYBERSECURITY INCIDENTS ARE INEVITABLE. OUR PREPAREDNESS WILL DETERMINE HOW WE RESPOND AND RECOVER. WE NEED TO DELINEATE A PLAN.

YOU'VE ALREADY BUILT SOLID CYBERSECURITY CAPABILITIES. THAT'S ESSENTIAL. AND WITH THE RIGHT STRATEGIES AND SUPPORT, AN INCIDENT'S IMPACT CAN BE MORE EFFECTIVELY MITIGATED.

FIRST, WE'LL CONDUCT A **RISK ASSESSMENT**. THIS WILL IDENTIFY CRITICAL ASSETS AND VULNERABILITIES AND PRIORITIZE EFFORTS AND ALLOCATE RESOURCES.

NEXT, WE'LL DEPLOY **ADVANCED THREAT DETECTION AND RESPONSE CAPABILITIES**, INCLUDING LEADING SECURITY TECHNOLOGIES AND THREAT INTELLIGENCE.

WITH THESE TOOLS, WE'LL CONDUCT REGULAR **TRAINING AND SIMULATIONS** TO KEEP SKILLS SHARP, AND TO BE SURE THAT YOU'RE PREPARED FOR A RANGE OF SCENARIOS. THIS WILL INCLUDE **TABLETOP EXERCISES AND FULL-SCALE SIMULATIONS**.

FINALLY, FOSTER A **CULTURE OF CYBERSECURITY AWARENESS** THROUGHOUT THE COMPANY, MAKING CYBERSECURITY A PART OF YOUR DAILY OPERATIONS, AND MAKING SURE THAT EVERYONE UNDERSTANDS THEIR ROLE IN PROTECTING COMPANY ASSETS.

EXCELLENT. I SAY WE MOVE FORWARD WITH THIS DETAILED APPROACH. ALL IN FAVOR?

THEN ONE DAY, SURE ENOUGH, IN THE IT DEPARTMENT...

WE'VE DETECTED AN ANOMALY!

IT LOOKS LIKE IT COULD BE FAR-REACHING. LET'S EXECUTE THE RESPONSE PLAN WE PRACTICED.

MEANWHILE, IN THE COMMUNICATIONS DEPARTMENT...

WE HAVE TO COMMUNICATE WITH OUR STAKEHOLDERS, EXTERNALLY AND INTERNALLY, SO THEY CAN DO THEIR PART TO HELP US CONTAIN THE THREAT.

BACK IN IT...

STATUS UPDATE?

HR SYSTEMS ARE BACK ONLINE. HERE COMES FINANCE ... WE'RE ALMOST THERE.

WE'VE ISOLATED THE THREAT. CONTAINMENT IS IN PROGRESS. SYSTEMS ARE STABILIZING.

GREAT JOB, EVERYONE. NEXT UPDATE IN AN HOUR.

THE MORNING AFTER...

THANKS TO OUR PREPAREDNESS, WE CONTAINED THE THREAT WITH MINIMAL IMPACT. HERE ARE THE LESSONS LEARNED AND OUR UPDATED MEASURES.

THESE UPDATES CAN FURTHER STRENGTHEN OUR DEFENSES AND IMPROVE OUR RESPONSE TIMES.

LEADERSHIP SHARES THE GOOD NEWS!

OUR RESILIENCE IS A TESTAMENT TO OUR PREPAREDNESS. LET'S CONTINUE TO PRIORITIZE CYBERSECURITY AND WORK TOGETHER TO PROTECT OUR ORGANIZATION.

CLAP

CLAP

CLAP

CLAP

CLAP

CLAP

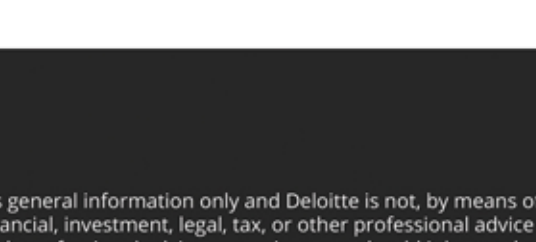
CLAP

END

HAPPILY EVER AFTER? NOT SO FAST! MORE INCIDENTS WILL COME, 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

About this publication

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

As used in this publication, "Deloitte" means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC. All rights reserved.