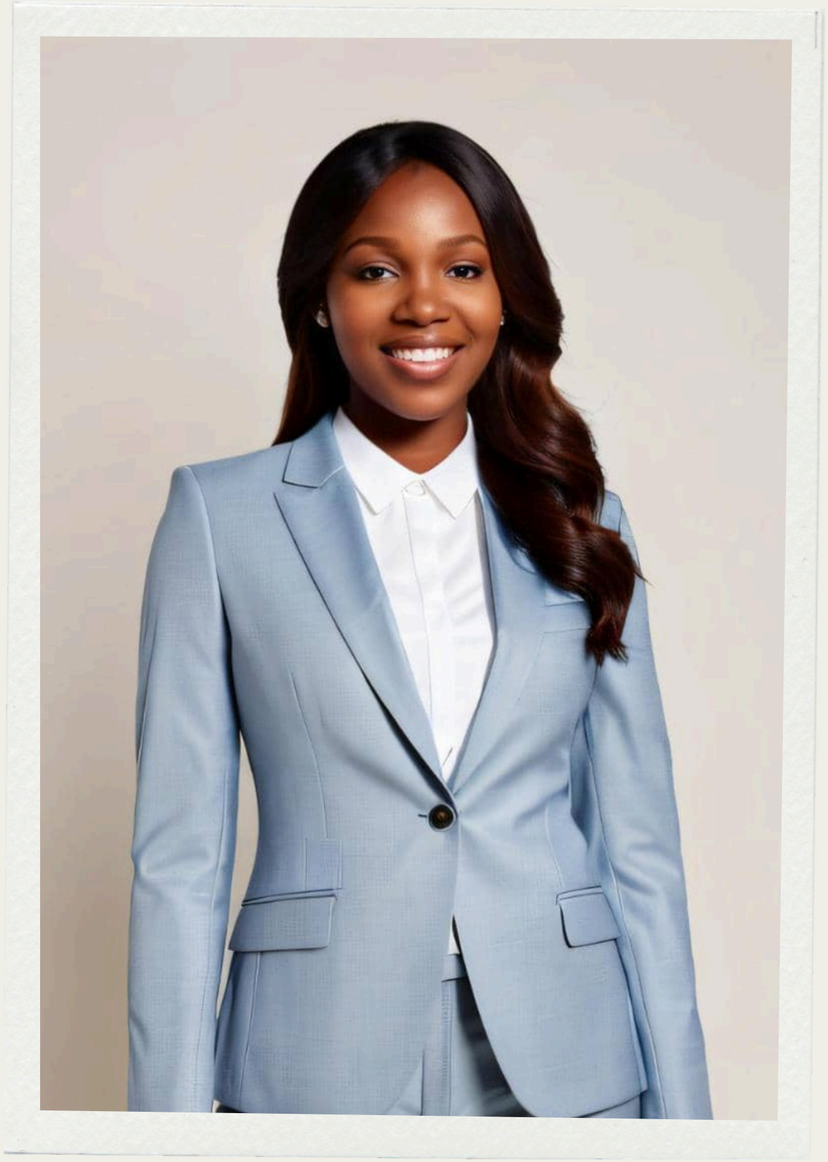


CYBER THREAT INTELLIGENCE, INCIDENT RESPONSE & MANAGEMENT

A STORY TELLING APPROACH

BLESSING IFEOLUWA OMOGBEHIN

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

STORY ONE

THE INSIDER THREAT

THE BETRAYAL

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

ACT 1: THE PREPARATION

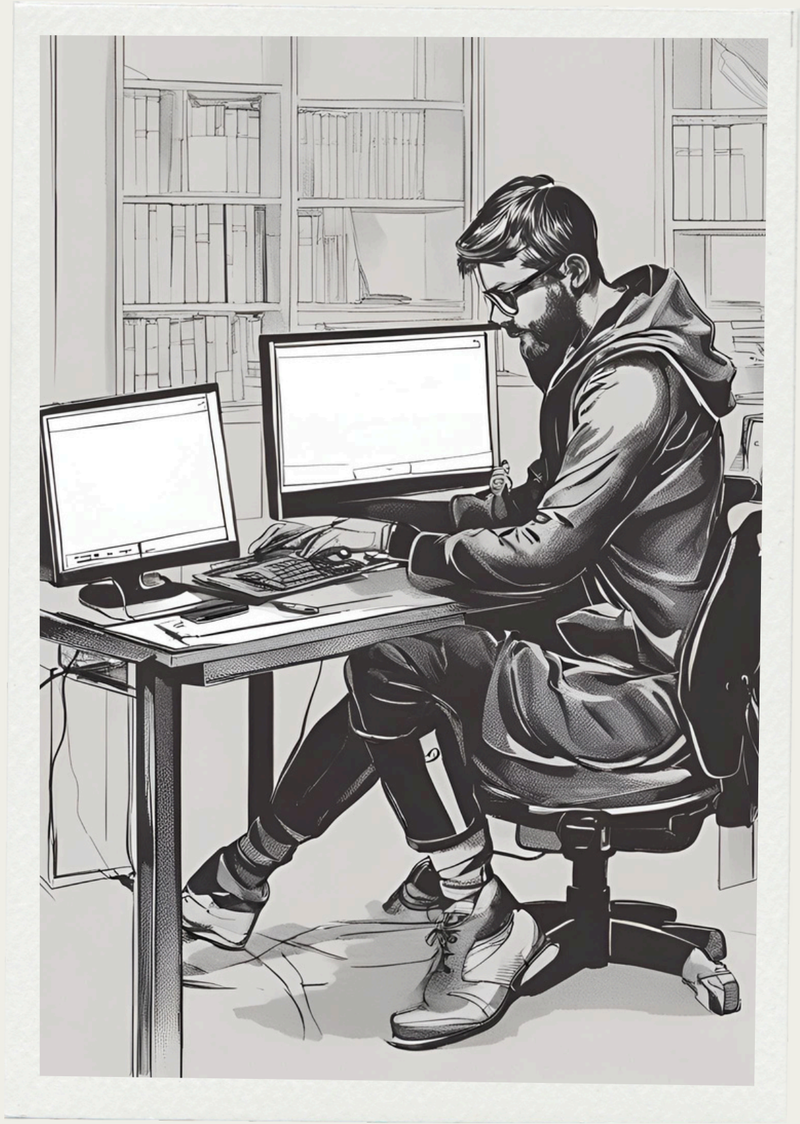
[SCENE: FUTUREMONEY INC. HEADQUARTERS – MORNING]

FUTUREMONEY INC., A LEADING FINANCIAL SERVICES COMPANY, IS KNOWN FOR ITS STRINGENT SECURITY MEASURES. THE OFFICE IS A HIVE OF ACTIVITY AS EMPLOYEES GO ABOUT THEIR TASKS. AMONG THEM IS JASON, A TRUSTED SENIOR ANALYST WITH FIVE YEARS AT THE COMPANY.

JASON (THINKING TO HIMSELF): ANOTHER DAY, ANOTHER DOLLAR. TIME TO GET STARTED.

JASON LOGS IN AND BEGINS HIS DAY, SIFTING THROUGH SENSITIVE FINANCIAL DATA. UNBEKNOWNST TO HIS COLLEAGUES, JASON IS STRUGGLING WITH MOUNTING PERSONAL DEBTS AND HAS BEEN APPROACHED BY A COMPETITOR OFFERING A SUBSTANTIAL PAYOFF FOR INSIDER INFORMATION.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA



ACT 2: THE BETRAYAL

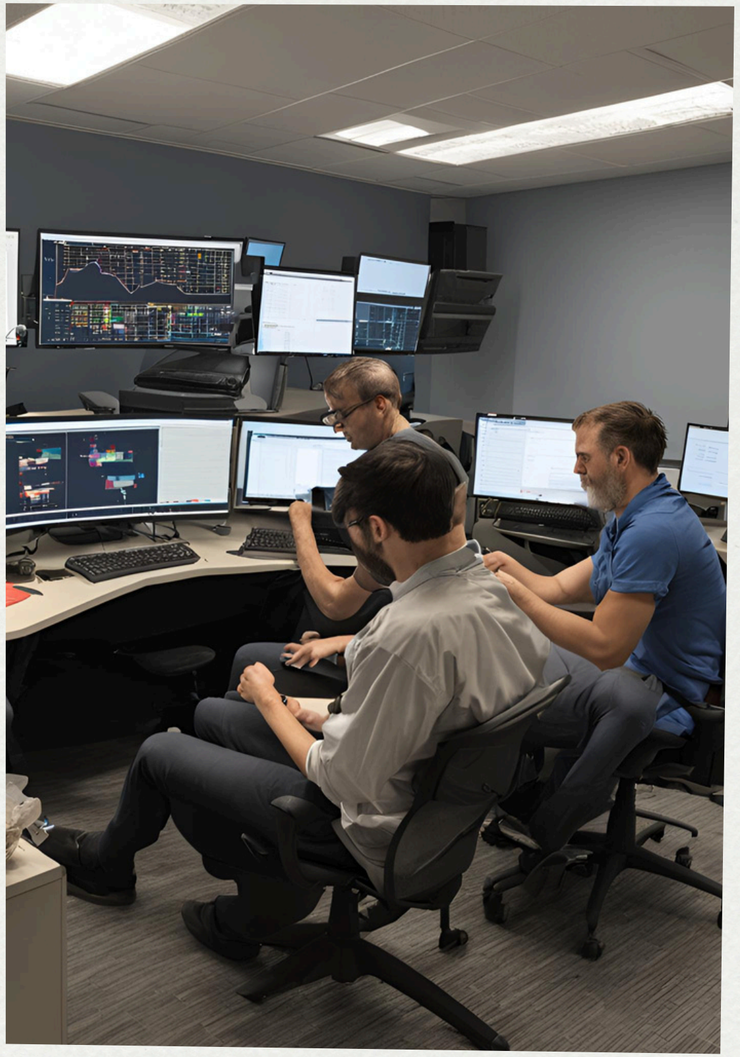
[SCENE: JASON'S APARTMENT – LATE NIGHT]

JASON SITS AT HIS COMPUTER, CONTEMPLATING THE CONSEQUENCES OF HIS ACTIONS. THE COMPETITOR'S OFFER IS TEMPTING, AND HIS FINANCIAL TROUBLES ARE OVERWHELMING.

JASON (MUTTERING TO HIMSELF): I DON'T HAVE A CHOICE. I NEED THE MONEY.

WITH A DEEP BREATH, HE LOGS INTO THE COMPANY'S SECURE DATABASE USING HIS CREDENTIALS. HE DOWNLOADS A TROVE OF CONFIDENTIAL CLIENT DATA AND FINANCIAL PROJECTIONS, CAREFULLY COVERING HIS TRACKS TO AVOID DETECTION.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA



ACT 3: THE DISCOVERY

[SCENE: FUTUREMONEY INC. SECURITY OPERATIONS CENTER – ONE WEEK LATER]

THE CYBERSECURITY TEAM AT FUTUREMONEY IS CONDUCTING ROUTINE MONITORING WHEN AN ANOMALY IS DETECTED. MARIA, THE HEAD OF CYBERSECURITY, NOTICES UNUSUAL ACCESS PATTERNS LINKED TO MICHAEL'S ACCOUNT.

MARIA: THIS DOESN'T LOOK RIGHT. WHY WOULD JASON NEED ACCESS TO THESE FILES?

SHE INITIATES A DEEPER INVESTIGATION, UNCOVERING A SERIES OF UNAUTHORIZED DOWNLOADS. THE TEAM QUICKLY REALIZES THE GRAVITY OF THE SITUATION.

MARIA: WE NEED TO ACT FAST. LOCK DOWN JASON'S ACCOUNT AND START A FORENSIC ANALYSIS IMMEDIATELY.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

ACT 4: THE FALLOUT

[SCENE: FUTUREMONEY INC. CONFERENCE ROOM – EMERGENCY MEETING]

THE EXECUTIVE TEAM GATHERS FOR AN URGENT MEETING. THE ATMOSPHERE IS TENSE AS THE SCALE OF THE BREACH BECOMES CLEAR.

CEO: HOW DID THIS HAPPEN UNDER OUR NOSES?

MARIA: JASON HAD LEGITIMATE ACCESS TO THE DATA, BUT HE ABUSED HIS PRIVILEGES. WE'VE IDENTIFIED THE DATA HE STOLE AND ARE WORKING TO CONTAIN THE BREACH.

CFO: WHAT'S THE IMPACT ON OUR CLIENTS?

MARIA: WE'RE STILL ASSESSING, BUT WE NEED TO INFORM THEM AND THE AUTHORITIES. THIS IS A SERIOUS BREACH OF TRUST.

JASON IS BROUGHT IN FOR QUESTIONING, LOOKING PALE AND DEFEATED.

CEO: WHY, JASON? WHY DID YOU DO IT?

JASON: I'M SO SORRY. I WAS DESPERATE. THE DEBT... IT WAS CRUSHING ME.

WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA
X.COM@BLESSINGOM001

ACT 5: THE CONCLUSION

[SCENE: FUTUREMONEY INC. HEADQUARTERS – THREE MONTHS LATER]

FUTUREMONEY HAS WEATHERED THE INITIAL STORM, BUT THE ROAD TO RECOVERY IS LONG. THE COMPANY HAS IMPLEMENTED NEW SECURITY MEASURES, FOCUSING ON INSIDER THREAT DETECTION AND RESPONSE.

MARIA (ADDRESSING THE TEAM): WE'RE INTRODUCING ENHANCED MONITORING FOR ALL EMPLOYEES, ESPECIALLY THOSE WITH ACCESS TO SENSITIVE DATA. WE'LL ALSO CONDUCT REGULAR AUDITS AND PROVIDE TRAINING ON RECOGNIZING AND REPORTING SUSPICIOUS BEHAVIOR.

THE SCREEN BEHIND MARIA DISPLAYS A NEW INSIDER THREAT DETECTION SYSTEM, DESIGNED TO IDENTIFY UNUSUAL ACCESS PATTERNS AND POTENTIAL RISKS.

CEO: OUR CLIENTS NEED TO KNOW WE'RE TAKING THIS SERIOUSLY. WE'RE OFFERING COMPLIMENTARY CREDIT MONITORING SERVICES AND ENSURING TRANSPARENCY THROUGHOUT THIS PROCESS.

THE TEAM NODS, DETERMINED TO REBUILD TRUST AND STRENGTHEN THEIR DEFENSES.

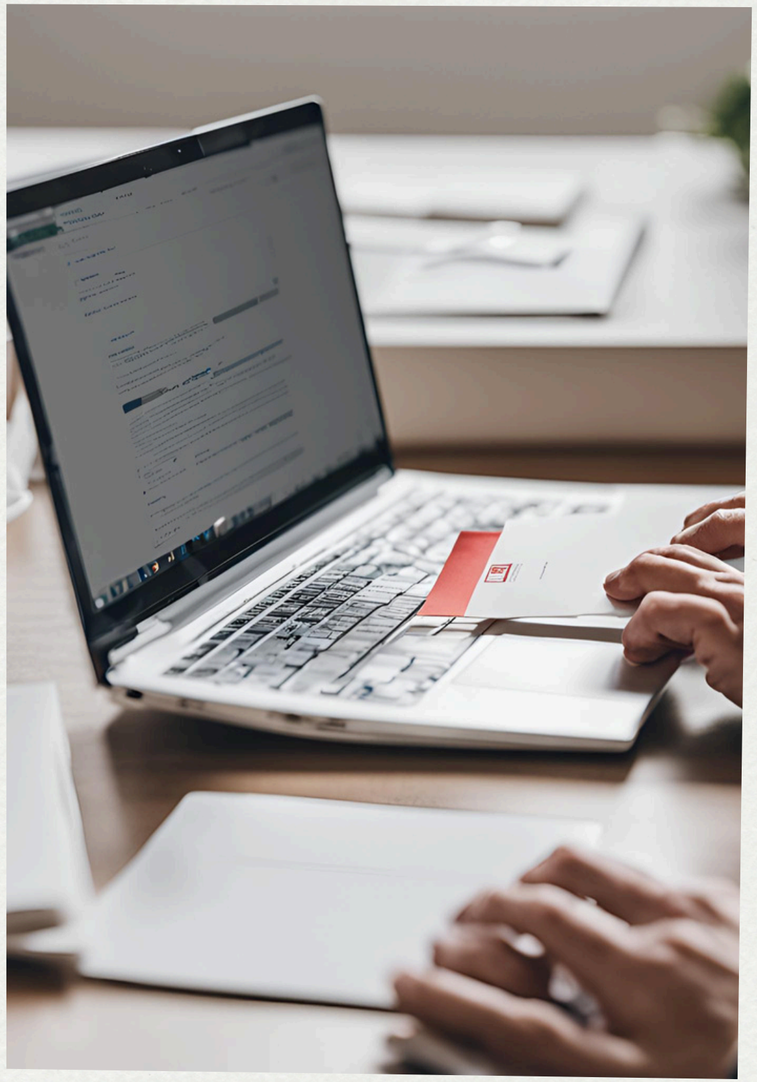
MARIA: REMEMBER, SECURITY IS EVERYONE'S RESPONSIBILITY. IF YOU SEE SOMETHING, SAY SOMETHING. WE'RE ALL IN THIS TOGETHER.

THE SCENE FADES OUT AS EMPLOYEES CONTINUE THEIR TRAINING, MORE VIGILANT AND UNITED THAN EVER.

STORY TWO

THE RANSOMWARE NIGHTMARE: A DIGITAL THREAT DRAMA

XBLESSINGOMo01
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA



ACT 1: THE VIRUS

[SCENE: CAREHEALTH SYSTEMS HEADQUARTERS – MORNING]

CAREHEALTH SYSTEMS, AN ACKNOWLEDGED HEALTHCARE PROVIDER, IS BUZZING WITH PATIENTS AND WORKERS. THE IT GROUP IS WORKING HARD TO KEEP THE HOSPITAL'S DIGITAL INFRASTRUCTURE RUNNING SMOOTHLY.
ESTHER, AN IT ADMINISTRATOR, RECEIVES AN EMAIL WITH THE SUBJECT "IMPORTANT UPDATE FOR MEDICAL SOFTWARE."

ESTHER (TO HERSELF): ANOTHER UPDATE? LET'S GET THIS DONE QUICKLY.

SHE OPENS THE EMAIL AND CLICKS ON THE LINK TO DOWNLOAD THE UPDATE. UNBEKNOWNST TO HER, THE EMAIL IS A SOPHISTICATED PHISHING ATTEMPT. THE LINK INSTALLS RANSOMWARE ONTO THE NETWORK. ESTHER NOTICES HER COMPUTER SCREEN FLICKER, THEN GO BLACK.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

ACT 2: THE REALIZATION

[SCENE: CAREHEALTH SYSTEMS IT DEPARTMENT – AFTERNOON]

CHAOS ERUPTS AS COMPUTERS ACROSS THE HOSPITAL NETWORK DISPLAY A MENACING MESSAGE: "YOUR FILES HAVE BEEN ENCRYPTED. PAY $5 MILLION IN BITCOIN TO DECRYPT." PANIC SPREADS AMONG THE STAFF AS PATIENT RECORDS AND CRITICAL SYSTEMS ARE LOCKED DOWN.

IT MANAGER: ESTHER, WHAT HAPPENED?

ESTHER: I THINK IT WAS THE UPDATE EMAIL. I'M SO SORRY, I DIDN'T REALIZE…

THE IT TEAM SCRAMBLES TO ASSESS THE DAMAGE AND FINDS THAT THE RANSOMWARE HAS SPREAD THROUGHOUT THE ENTIRE NETWORK, AFFECTING PATIENT RECORDS, BILLING SYSTEMS, AND EVEN MEDICAL EQUIPMENT.

ACT 3: THE IMPACT

[SCENE: CAREHEALTH SYSTEMS EMERGENCY MEETING – EVENING]

THE EXECUTIVE TEAM GATHERS IN A STATE OF URGENCY. THE CEO, DR. VICTOR, LOOKS GRIM.

DR. VICTOR: WE'RE IN A CRITICAL SITUATION. PATIENTS' LIVES ARE AT RISK. WHAT ARE OUR OPTIONS?

IT MANAGER: WE HAVE BACKUPS, BUT IT WILL TAKE TIME TO RESTORE EVERYTHING. THE RANSOM DEMAND IS $5 MILLION, AND THEY'RE GIVING US 48 HOURS.

COO: PAYING THE RANSOM ISN'T A GUARANTEE. WE CAN'T TRUST CRIMINALS.

CISO: WE NEED TO CONTACT LAW ENFORCEMENT AND OUR CYBERSECURITY INSURANCE PROVIDER. IN THE MEANTIME, WE SHOULD FOCUS ON RESTORING ESSENTIAL SERVICES FROM BACKUPS.
DR. VICTOR NODS, HIS FACE RESOLUTE.

DR. VICTOR: DO WHATEVER IT TAKES. OUR PATIENTS COME FIRST.

ACT 4: THE RECOVERY

[SCENE: CAREHEALTH SYSTEMS – THREE DAYS LATER]

THE IT TEAM WORKS AROUND THE CLOCK TO RESTORE SYSTEMS FROM BACKUPS. CRITICAL PATIENT CARE SYSTEMS ARE PRIORITIZED. THE FBI IS INVOLVED, INVESTIGATING THE ATTACK.

ESTHER (TO THE IT MANAGER): WE'VE RESTORED 60% OF OUR SYSTEMS, BUT IT'S SLOW GOING. AT LEAST PATIENT RECORDS ARE BACK ONLINE.

IT MANAGER: GOOD WORK. KEEP PUSHING. EVERY HOUR COUNTS.

DR. VICTOR ADDRESSES THE STAFF, REASSURING THEM AND THE PATIENTS.

DR. VICTOR: WE ARE MAKING PROGRESS. THANK YOU FOR YOUR PATIENCE AND DEDICATION DURING THIS CRISIS. OUR PRIMARY FOCUS REMAINS THE SAFETY AND CARE OF OUR PATIENTS.

ACT 5: THE LESSONS LEARNED

[SCENE: CAREHEALTH SYSTEMS HEADQUARTERS – ONE MONTH LATER]

THE HOSPITAL IS OPERATING NORMALLY AGAIN, BUT THE EXPERIENCE HAS LEFT A LASTING IMPACT. A COMPANY-WIDE MEETING IS CALLED TO DISCUSS THE INCIDENT AND THE MEASURES BEING IMPLEMENTED TO PREVENT FUTURE ATTACKS.

DR. VICTOR: WE'VE LEARNED A HARD LESSON, BUT WE'RE STRONGER FOR IT. HERE'S WHAT WE'RE DOING MOVING FORWARD.

THE CISO OUTLINES THE NEW SECURITY MEASURES.

CISO: WE'RE IMPLEMENTING ADVANCED THREAT DETECTION AND RESPONSE SYSTEMS. ALL STAFF WILL UNDERGO MANDATORY CYBERSECURITY TRAINING, FOCUSING ON RECOGNIZING PHISHING ATTEMPTS AND OTHER THREATS. THE SCREEN BEHIND THE CISO DISPLAYS NEW SECURITY PROTOCOLS AND SOFTWARE.

CISO: WE'RE ALSO ENHANCING OUR BACKUP PROCEDURES AND ENSURING THEY ARE TESTED REGULARLY. MULTI-FACTOR AUTHENTICATION WILL BE REQUIRED FOR ALL CRITICAL SYSTEMS ACCESS.

DR. VICTOR: REMEMBER, SECURITY IS A SHARED RESPONSIBILITY. WE MUST ALL STAY VIGILANT TO PROTECT OUR PATIENTS AND OUR SYSTEMS.

THE STAFF NODS, DETERMINED TO UPHOLD THE NEW STANDARDS. THE SCENE SHIFTS TO A CYBERSECURITY TRAINING SESSION, WHERE EMPLOYEES LEARN ABOUT THE LATEST THREATS AND HOW TO RESPOND.

NARRATOR: CAREHEALTH SYSTEMS TURNED A RANSOMWARE NIGHTMARE INTO A WAKE-UP CALL, STRENGTHENING THEIR DEFENSES AND FOSTERING A CULTURE OF CYBERSECURITY AWARENESS. THROUGH VIGILANCE, TRAINING, AND ADVANCED TECHNOLOGY, THEY ENSURED THEIR COMMITMENT TO PATIENT SAFETY AND DATA SECURITY REMAINED UNBROKEN.

X.COM@BLESSINGOM001

STORY THREE

THE SUPPLY CHAIN INFILTRATION: A DRAMA OF HIDDEN VULNERABILITIES

X.COM@BLESSINGOM001

ACT 1: THE PARTNERSHIP

[SCENE: TECHNOW INNOVATIONS HEADQUARTERS – MORNING]

TECHNOW INNOVATIONS, A LEADING TECH COMPANY SPECIALIZING IN SMART HOME DEVICES, IS THRIVING. THE OFFICE IS BUZZING WITH EXCITEMENT AS THEY ANNOUNCE A NEW PARTNERSHIP WITH SECURESOFT, A SOFTWARE VENDOR PROVIDING KEY COMPONENTS FOR TECHNOWT'S FLAGSHIP PRODUCT.

CEO, JULIET: THIS PARTNERSHIP WITH SECURESOFT WILL TAKE OUR PRODUCT TO THE NEXT LEVEL. LET'S GET THEIR SOFTWARE INTEGRATED AS SOON AS POSSIBLE.

THE IT TEAM, LED BY FRANK, BEGINS THE INTEGRATION PROCESS, EAGER TO LEVERAGE SECURESOFT'S CAPABILITIES. EVERYTHING SEEMS TO BE PROGRESSING SMOOTHLY.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

ACT 2: THE HIDDEN THREAT

[SCENE: TECHNOW INNOVATIONS IT DEPARTMENT – LATE EVENING]

FRANK STAYS LATE TO FINALIZE THE SOFTWARE INTEGRATION. AS HE TESTS THE NEW SYSTEM, HE NOTICES UNUSUAL ACTIVITY ON THE NETWORK.

FRANK (TO HIMSELF): THAT'S ODD. WHY IS THERE SO MUCH OUTBOUND TRAFFIC?

HE DIGS DEEPER AND DISCOVERS THAT THE SOFTWARE UPDATE FROM SECURESOFT HAS OPENED A BACKDOOR INTO TECHNOW'S NETWORK. THE BACKDOOR IS BEING EXPLOITED BY A SOPHISTICATED HACKING GROUP.

FRANK: THIS IS NOT POSSIBLE. I NEED TO ALERT THE TEAM IMMEDIATELY.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

ACT 3: THE INFILTRATION

[SCENE: TECHNOW INNOVATIONS HEADQUARTERS – EMERGENCY MEETING]

THE NEXT MORNING, THE EXECUTIVE TEAM GATHERS FOR AN EMERGENCY MEETING. THE ATMOSPHERE IS TENSE AS FRANK EXPLAINS THE SITUATION.

FRANK: THE SOFTWARE WE INTEGRATED FROM SECURESOFT CONTAINS A BACKDOOR. HACKERS ARE USING IT TO SIPHON OUR DATA.

CEO, JULIET: HOW COULD THIS HAPPEN? WE VETTED THEIR SECURITY PROTOCOLS.

CISO, ANNA: SUPPLY CHAIN ATTACKS ARE BECOMING MORE COMMON. IT'S LIKELY THAT SECURESOFT'S SYSTEMS WERE COMPROMISED WITHOUT THEIR KNOWLEDGE. WE NEED TO ACT FAST TO CONTAIN THIS.

CTO, MARK: WHAT'S OUR PLAN TO MITIGATE THIS?

FRANK: WE'RE ISOLATING THE COMPROMISED SYSTEMS AND WORKING ON PATCHING THE VULNERABILITIES. WE ALSO NEED TO NOTIFY SECURESOFT AND COLLABORATE ON A RESOLUTION.

ACT 4: THE RESPONSE

[SCENE: TECHNEW INNOVATIONS IT DEPARTMENT – CONTINUOUS OPERATION]

THE IT TEAM WORKS AROUND THE CLOCK TO CONTAIN THE BREACH. COMMUNICATION WITH SECURESOFT REVEALS THAT THEY WERE UNAWARE OF THE COMPROMISE.

FRANK: SECURESOFT IS WORKING ON THEIR END TO IDENTIFY AND ELIMINATE THE BACKDOOR. WE'VE STARTED A FULL NETWORK AUDIT AND ENHANCED OUR MONITORING SYSTEMS.

ANNA: WE'RE ALSO IMPLEMENTING STRICTER CONTROLS FOR THIRD-PARTY INTEGRATIONS. EVERY PIECE OF SOFTWARE WILL UNDERGO RIGOROUS SECURITY TESTING BEFORE DEPLOYMENT.

AS THE DAYS PASS, THE TEAM MAKES SIGNIFICANT PROGRESS IN SECURING THEIR SYSTEMS AND PREVENTING FURTHER DATA LOSS.

ACT 5: THE RESOLUTION

[SCENE: TECHNEW INNOVATIONS HEADQUARTERS – ONE MONTH LATER]

TECHNEW HAS SUCCESSFULLY CONTAINED THE BREACH AND IS NOW FOCUSED ON STRENGTHENING ITS DEFENSES. THE EXECUTIVE TEAM MEETS TO DISCUSS THE LESSONS LEARNED AND THE STEPS FORWARD.

CEO, JULIET: THANKS TO EVERYONE'S HARD WORK, WE'VE NAVIGATED THROUGH THIS CRISIS. WE MUST ENSURE THIS NEVER HAPPENS AGAIN.

ANNA OUTLINES THE NEW SECURITY MEASURES BEING IMPLEMENTED.

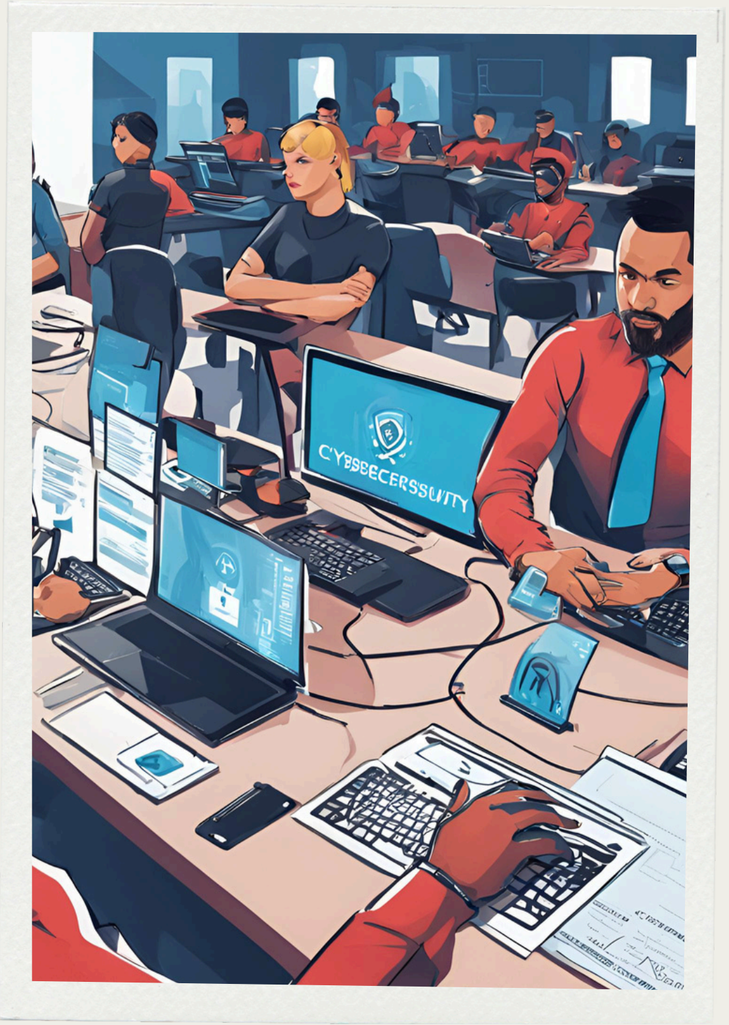
ANNA: WE'RE ESTABLISHING A COMPREHENSIVE VENDOR RISK MANAGEMENT PROGRAM. THIS INCLUDES CONTINUOUS MONITORING OF THIRD-PARTY SOFTWARE AND STRICTER ACCESS CONTROLS.

FRANK: WE'RE ALSO CONDUCTING REGULAR CYBERSECURITY TRAINING FOR ALL EMPLOYEES, EMPHASIZING THE IMPORTANCE OF VIGILANCE WHEN DEALING WITH THIRD-PARTY VENDORS.

MARK: AND OUR COLLABORATION WITH SECURESOFT?

ANNA: SECURESOFT HAS IMPLEMENTED THEIR OWN ENHANCED SECURITY MEASURES. WE'LL MAINTAIN A CLOSE PARTNERSHIP TO ENSURE MUTUAL SECURITY.

THE SCENE SHIFTS TO A TRAINING SESSION, WHERE EMPLOYEES ARE LEARNING ABOUT THE NEW PROTOCOLS AND THE IMPORTANCE OF SUPPLY CHAIN SECURITY.



NARRATOR: TECHNEW INNOVATIONS TRANSFORMED A POTENTIALLY DISASTROUS DISTRIBUTION SYSTEM ATTACK INTO A CHANCE FOR DEVELOPMENT AND PROGRESS. THEY STRENGTHENED THEIR DEFENCES AGAINST FUTURE ATTACKS BY PUTTING IN PLACE STRICT SECURITY PROCEDURES, CULTIVATING SOLID ALLIANCES, AND EDUCATING THEIR WORKERS.

X.COM@BLESSINGOM001
WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

CYBERSECURITY CONTENTS COVERED IN STORIES

- INSIDER THREATS
- CYBER THREAT INTELLIGENCE
- RANSOMEWARE
- BACKDOOR ATTACK
- INCIDENT RESPONSE
- INCIDENT RESPONSE TEAM
- INCIDENT MANAGEMENT
- DISASTER RECOVERY
- THE ROLE OF SOC
- BUSINESS CONTINUITY
- ACCESS CONTROL E.T.C.

WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA

MANY THANKS FOR READING!

LIKE, COMMENT & REPOST.
LET US GROW A COMMUNITY & NATION FULL OF CYBERSECURITY LITERATES

WWW.LINKEDIN.COM/IN/OMOGBEHINBLESSINGIFEOLUWA