GenSys Breach Response – Film Script

Cast Assignments

Each role is portrayed by a member of the project team (camera operator Aiz Anches is off-camera):

- **Amorin Elmer**: Chief Information Officer (CIO)
- **Christian Butaya**: Chief Security Officer (CSO)
- **Clyde Parol**: IT Manager
- **Elmer Amorin**: Ethics Officer
- **Glenn Biboso**: Public Relations (PR) Officer
- **Jacob John Paguta**: Media Journalist
- **Jan Nichols Maristela**: Angry Citizen
- **Jan Nichols Nguyen Maristela**: Internal Whistleblower
- **Jesse Ray Zarate Morcillos**: Data Privacy Officer
- **Kristopher V. Dichos**: Government Health Secretary
- **Layca Bahandi Cantalado**: Concerned Citizen 1
- **Richard Shane Gamon**: Concerned Citizen 2

Opening Context & Hacker Scene

Opening montage: A series of quick news clips about recent data breaches flashes across the screen. Headlines like “Major Medical Provider Hacked” and “Millions of Records Exposed” set the stakes. A voice-over warns that data has become the currency of the modern world.

Scene 0 – The Hackers: In a dark room lit by computer monitors, three hackers sit at laptops. They talk quietly while code scrolls down their screens.

Hacker 1: “Okay, guys, I found something interesting. GenSys is still running an older firewall. No two-factor authentication on admin accounts.”

Hacker 2: “Public health data? That’s gold. Get in, grab everything and we’ll sell it.”

Hacker 3: “Running a brute-force script now. They’re using ‘admin123’ as a password. This is too easy.”

Hacker 1: “We’re in! I’m seeing names, addresses, medical histories. It’s like they’re begging to be hacked.”

Hacker 2: “Move fast. Copy the data and wipe our traces before anyone notices.”

Hacker 3: “Done. Our buyer is ready. Let’s get paid.”

The hackers leave quickly. A caption notes: *“12 hours later, GenSys discovers the breach.”*

Act I – Emergency Meeting

Setting: A modern conference room inside GenSys headquarters. Leadership and key staff gather around a table, copies of the breach report in hand.

CIO (Amorin): “Thank you for coming on such short notice. We’ve suffered a breach – more than 10,000 records were compromised. Christian, can you tell us what happened?”

CSO (Christian): “Attackers exploited our outdated firewall and weak admin passwords. They slipped in and took data before we detected the intrusion.”

IT Manager (Clyde): “We can restore and secure the system in forty-eight hours. We’re patching the firewall and enforcing multi-factor authentication.”

Ethics Officer (Elmer): “These aren’t just numbers. These are people’s lives. We need to notify them and support them.”

PR Officer (Glenn): “We’ll craft a clear statement. We can’t hide the breach, but we can control how we communicate it.”

Data Privacy Officer (Jesse): “We’re legally obligated to inform regulators and victims. Delaying could make things worse.”

Government Secretary (Kristopher): “We need to manage the technical fix, legal fallout and public trust all at once. Amorin, what’s your plan?”

CIO (Amorin): “We contain the breach, investigate, notify everyone and hold a press briefing. We need to work as one.”

The team debates the timeline and divides responsibilities, showing urgency and concern. They agree to hold a press conference in 36 hours.

Act II – Press Conference

Setting: A mock press room with a podium and backdrop. Cameras and reporters are ready.

PR Officer (Glenn): “Good afternoon. GenSys recently detected a cyber-attack accessing more than ten thousand records. We shut down the affected servers and launched an investigation. We deeply regret this incident and will support all affected individuals.”

(Glenn looks up.)

PR Officer (Glenn): “We will now take questions.”

Journalist (Jacob): “Why did you wait more than a day to inform the public?”

PR Officer (Glenn): “We wanted to confirm the facts before going public. We weren’t hiding; we were ensuring accuracy.”

CIO (Amorin): “Transparency is our goal, but we needed solid information first.”

Journalist (Jacob): “What failed? Were you unaware of the outdated firewall?”

CSO (Christian): “Our firewall was outdated and some admin passwords were weak. We own that mistake and are fixing it now.”

Journalist (Jacob): “Will anyone be held accountable? Are you offering compensation?”

Ethics Officer (Elmer): “We’re focusing on systemic change, but accountability matters. We’ll also offer free identity-theft monitoring and cover any losses.”

Data Privacy Officer (Jesse): “We notified regulators promptly and are cooperating fully. We’ll share findings as soon as they are verified.”

(A note is slipped to Jacob from an unidentified person. He glances at it.)

Journalist (Jacob): “One last question: did your own employees warn you about security risks months ago?”

CIO (Amorin): “If warnings were raised and ignored, we will investigate and ensure that never happens again.”

The press conference wraps up amid murmurs and scribbling reporters, hinting that a deeper issue may be exposed.

Act III – Community Forum

Setting: A public hall filled with concerned citizens and the media. The GenSys team sits at a panel facing the audience.

Angry Citizen (Jan Nichols): “My husband’s medical history is now floating around the internet. Why should we ever trust you again?”

CIO (Amorin): “We failed to protect your data. We can’t erase that, but we can own it and do

better. Rebuilding trust will take time and action."

Concerned Citizen 1 (Layca): "How will you ensure this never happens again?"

IT Manager (Clyde): "We're overhauling our security infrastructure, introducing stronger firewalls and multi-factor authentication, and hiring external auditors to review our systems."

Concerned Citizen 2 (Richard): "What about compensation? Some of us might suffer financial losses."

Ethics Officer (Elmer): "We're offering credit and identity-monitoring services and a compensation fund for any verified losses."

Data Privacy Officer (Jesse): "We're creating an oversight committee that includes community representatives so you have a voice in our security decisions."

(A figure stands up in the back.)

Whistleblower (Jan Nguyen): "I worked on your security team. Months ago, we warned management about the outdated firewall and weak passwords. We were ignored because of budget concerns. Now everyone is paying for that."

CSO (Christian): "I admit we delayed the upgrades. It was a mistake driven by cost fears. I'm sorry."

Government Secretary (Kristopher): "We'll launch an investigation into why those warnings were ignored and establish a formal whistleblower program. It shouldn't have taken this long or gone this far."

CIO (Amorin): "Thank you for speaking up. Your courage helps us become better and more accountable."

The forum continues with more questions and apologies, but the mood shifts as the truth emerges and commitments to change are made.

Act IV – Debrief & Reflection

Setting: Backstage or in a classroom. The cast members step out of character to discuss their experience.

Director: "Let's talk about how that felt. Christian?"

CSO (Christian): "Admitting failure was tough. But being honest about mistakes is essential in a crisis."

Ethics Officer (Elmer): “Playing the empathy role reminded me that there are real people behind the data.”

PR Officer (Glenn): “It was tricky to communicate bad news without sounding robotic. Being straightforward felt most genuine.”

CIO (Amorin): “Balancing technical fixes, legal duties and public trust felt overwhelming. It mirrored real-world leadership challenges.”

Whistleblower (Jan Nguyen): “Speaking up against management felt empowering. Organisations need to listen to their people before it’s too late.”

Data Privacy Officer (Jesse): “We learned that efficiency without ethics can cause harm, and ethics without efficiency can stall progress. Both are needed.”

Government Secretary (Kristopher): “Budgets and bureaucracy can’t be excuses for neglecting security. Real lives are affected.”

Director: “What can we apply from this to real life?”

Group: “Listen to warnings early, balance empathy with action, and be transparent. It’s not just about fixing systems; it’s about protecting people.”

The discussion continues informally as the group reflects on their roles, connecting the exercise to real-world incidents and the importance of proactive security and ethical leadership.