Post Incident Review

Simulated Incident Response for mini-sprint event by CLICKED - IBM

MAVEN

Post Incident Review

A **security incident** has been detected in Maven’s IT infrastructure, **compromising patient data** and **system integrity**

Today’s Goal

Understand What has happened

The impact on business

Action Taken

Lesson Learn - Prevention & Est.Budget

Timeline

Sep 20 03:15 pm (PST)

Initial compromise detected

Sep 20-Sep 22

Isolated the compromised system

Deleted malicious program

Restored patient data from backup

Sep 22 12:30 (PST)

Back to normal operation

September 22 8:00 am (PST)

Security experts from NoMoreAttack Inc entered site and conducted forensic analysis

03:00 pm (PST)

Found more than 500 patients data is likely to be impacted by Chinese Hacker Group “No Mercy”

Sep 23 12:00 pm (PST)

Issued press release about incident

Sep 24 12:00 pm (PST)

Call-center started operation

Security Review

What Went Right

1. **Quick detection** of the initial suspicious data exfiltration
2. **Successful blocking** of potential data exfiltration attempt via DNS
3. **Rapid response and containment** once the incident was fully identified

Security Review

Areas for Improvement

1. **Inadequate monitoring** of admin-level activities and policy changes
2. **Insufficient Account Access Management,** allowing lateral movement attempts

Business Impact

System downtime (containment & recovery)

Overtime work for many employees

Fines for regulatory non-compliance

Loss of trust by public

Business Impact

Overtime Hours (Sep 20-25)	Service fee NoMoreAttack Inc	HIPAA violation	Establish and maintain Call Center	Business interruption
Total Over Time Cost $37,000	$30,000	Fine up to $50,000	$50,000	$100,,000
Senior Manager: 40 hours System Analyst: 60 hours System Admin: 10 hours Legal department: 50 hours PR department: 50 hours	Per this Incident	Per Violation	Agent service for 3 months:	Business stopped for 1.5 days

Total Cost: $277,000

Business Impact

Although **cyber liability insurance** covers most expenses (Up to $5 million), **reputation damage** hurt Maven Clinic

Preventative measures

Lessons Learned

PEOPLE

Incident Response & Security Awareness Training

PROCESS

Privilege Management

TECHNOLOGY

System Monitoring

Future Budget

Total Budget: $262,000 for Q1, 2024

Incident Response Training (70 employees) People	Security Awareness Training (70 employees) People	Privilege Management (Process)	XDR Tool (Technology)	Security Analyst (Technology)
Incident response training (3 hours/year) Training Coach $5,000	Implement e-learning platform $10,000/year	Hire an IAM professional $120,000/year	100 Endpoint /$7200/year/ SentinelOne	Hire a Security Analyst professional $120,000/year
Provide incident response training to employees with assigned roles and responsibilities	Conduct security awareness training to raise awareness that they are the front-line defense	Adapting least privilege principles, zero trust and manage user accounts to mitigate the risk of privilege escalation	Implement a monitoring system to detect attacks and indicators of potential attacks	Manage related rules and monitor

Thank you