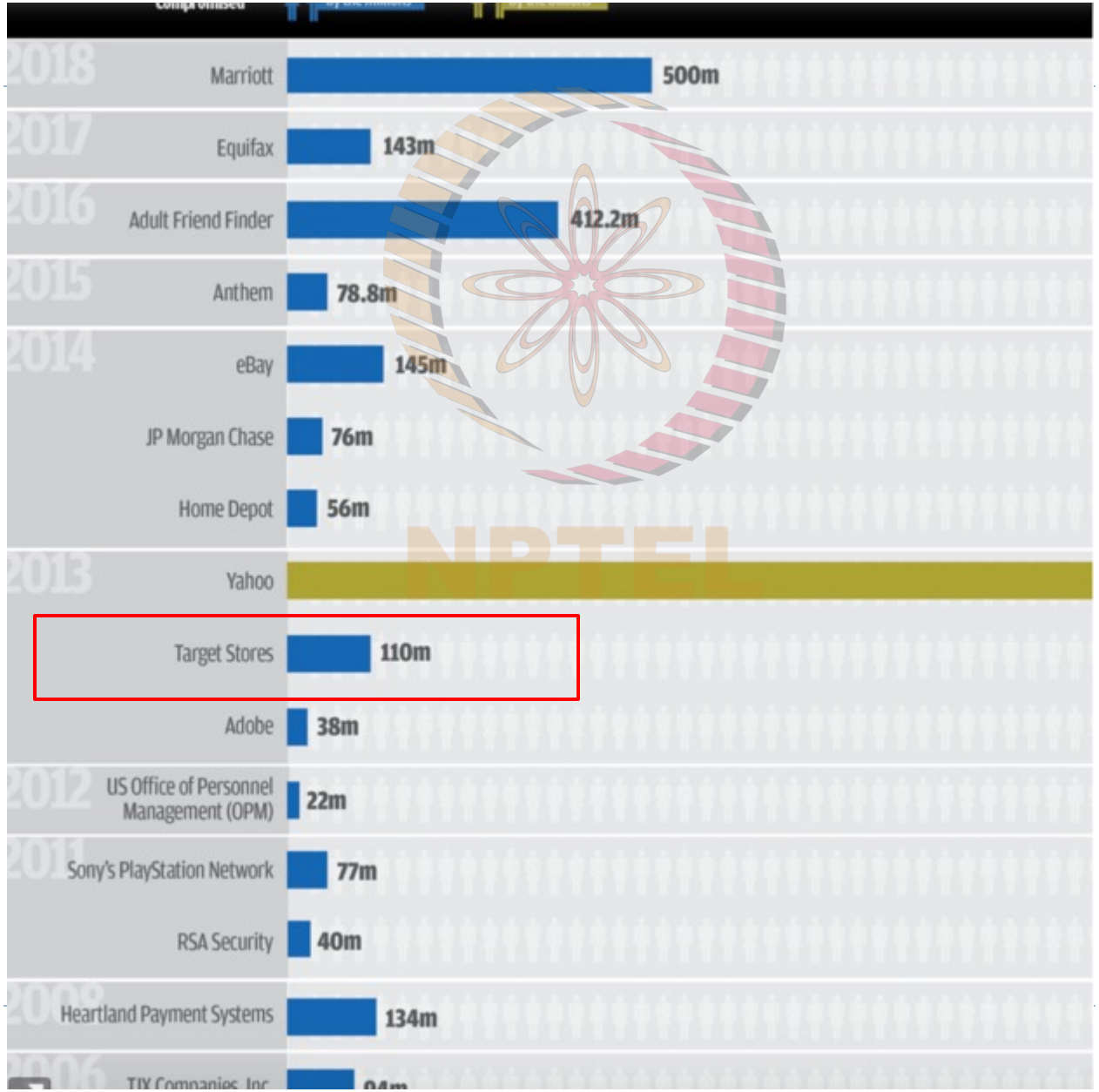
Cyber Security and Privacy
MS6880

Governance, Risk and Compliance

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

Major data breaches




FORTUNE FAVORS
THE PREPARED
MIND.
LOUIS PASTEUR

Approaches to cyber security management

- Governance-Risk-Compliance (GRC) approach
  - Dominant accounting/finance perspective
  - Cyber security management as an *internal control* mechanism
- Standards driven approach
  - NIST cyber security framework (open)
  - ISO/IEC 27001 for information security (proprietary)
- Organizational planning approach
  - Cyber security as a part of strategic planning and risk management
  - Contingency planning a constituent of the approach

GRC approach: Control frameworks

Widespread accounting fraud in the late 90's to early 2000 resulted in mandatory reforms to prevent fraud

- COBIT: Control Objectives of Information Related Technology
  - Framework for *IT control*
  - Specified by ISACA (Information Systems Audit and Control Association)
- COSO: Committee of Sponsoring Organizations
  - Framework for enterprise *internal controls* (control-based approach)
  - Specified by American Accounting Association and others
- COSO-ERM (Enterprise Risk Management)
  - Expands COSO framework taking a risk-based approach

Internal controls

- Processes implemented to provide assurance that the following objectives are achieved:
  - Safeguard assets
  - Maintain sufficient records
  - Provide accurate and reliable information
  - Prepare financial reports according to established criteria
  - Promote and improve operational efficiency
  - Encourage adherence with management policies
  - Comply with laws and regulations

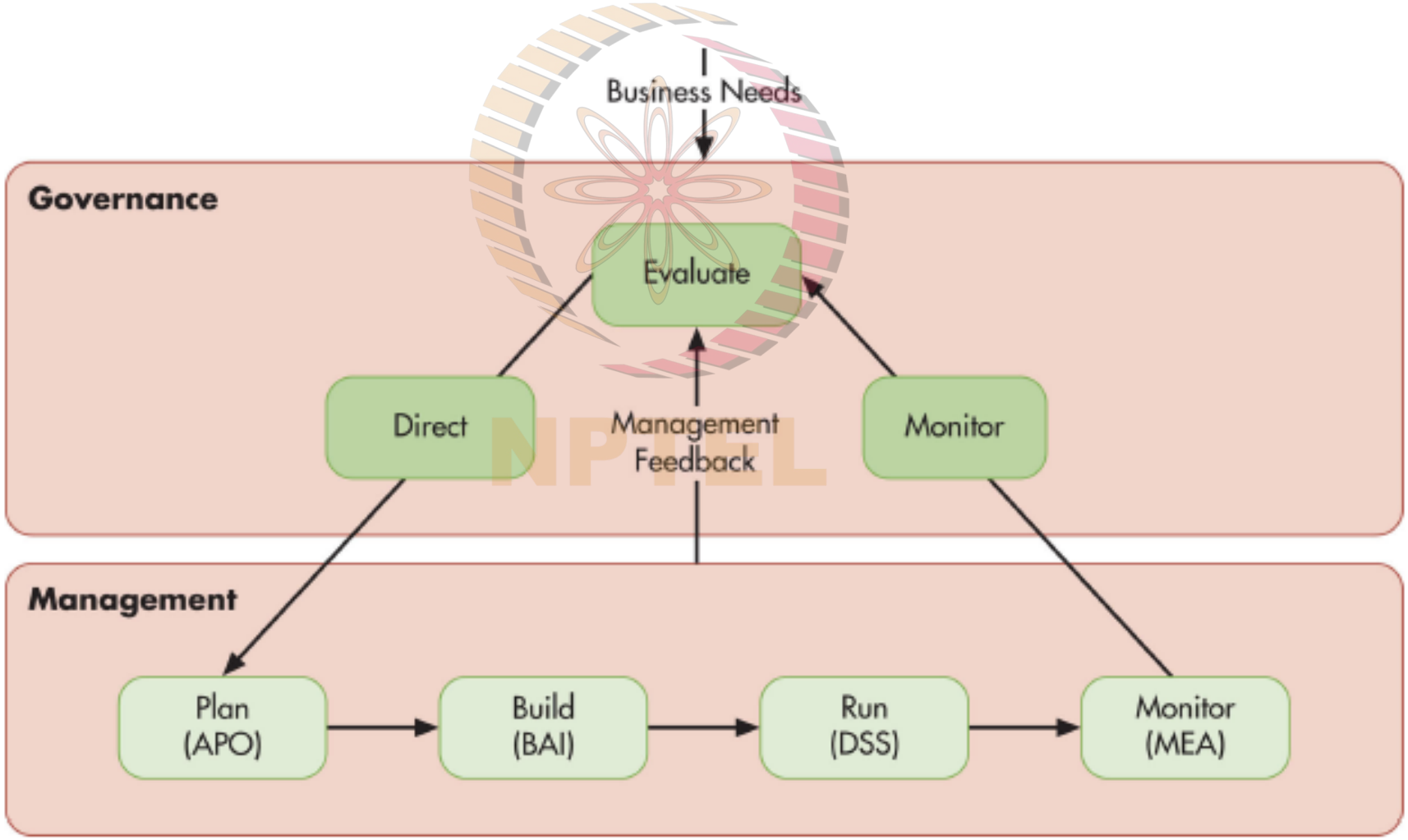
Functions of internal controls

- Preventive controls
  - Deter problems from occurring
- Detective controls
  - Discover problems that are not prevented
- Corrective controls
  - Identify and correct problems; correct and recover from the problems

COBIT framework

- Current framework version is COBIT 5
- Based on the following principles:
  - Meeting stakeholder needs
  - Covering the enterprise end-to-end
  - Applying a single, integrated framework
  - Enabling a holistic approach
  - Separating governance from management

COBIT 5 Separates Governance from Management



Components of COSO Frameworks

COSO

- Control (internal) environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

COSO-ERM

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Standards: ISO/IEC 17799:2005

- One of the most widely referenced and often discussed security models is Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- The purpose is to establish "guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization"

ISO 27000 series

- ISO/IEC 17799:2005 has 133 possible controls, not all of which must be used; part of the process is to identify which are relevant
- Each section includes four categories of information:
  - One or more objectives
  - Controls relevant to the achievement of the objectives
  - Implementation guidance
  - Other information
- Renamed as ISO 27002 in 2007
- ISO 27001 provides guidelines on implementation (PDCA format)

Published standards [edit]

The published ISO27K standards related to "information technology - security techniques" are:

1. ISO/IEC 27000 — Information security management systems — Overview and vocabulary[9]
2. ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements. The 2013 release of the standard specifies an information security management system in the same formalized, structured and succinct manner as other ISO standards specify other kinds of management systems.
3. ISO/IEC 27002 — Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS
4. ISO/IEC 27003 — Information security management system implementation guidance
5. ISO/IEC 27004 — Information security management — Monitoring, measurement, analysis and evaluation[10]
6. ISO/IEC 27005 — Information security risk management[11]
7. ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
8. ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on auditing the management system)
9. ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on auditing the information security controls)
10. ISO/IEC 27009 — Essentially an internal document for the committee developing sector/industry-specific variants or implementation guidelines for the ISO27K standards
11. ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications
12. ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
13. ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (derived from ITIL)
14. ISO/IEC 27014 — Information security governance.[12] Mahncke assessed this standard in the context of Australian e-health.[13]
15. ISO/IEC TR 27015 — Information security management guidelines for financial services - Now withdrawn[14]
16. ISO/IEC TR 27016 — information security economics
17. ISO/IEC 27017 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
18. ISO/IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
19. ISO/IEC TR 27019 — Information security for process control in the energy industry
20. ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity

22. ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts
23. ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security
24. ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
25. ISO/IEC 27033-4 — Network security - Part 4: Securing communications between networks using security gateways
26. ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
27. ISO/IEC 27033-6 — Network security - Part 6: Securing wireless IP network access
28. ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security
29. ISO/IEC 27034-2 — Application security - Part 2: Organization normative framework
30. ISO/IEC 27034-6 — Application security - Part 6: Case studies
31. ISO/IEC 27035-1 — Information security incident management - Part 1: Principles of incident management
32. ISO/IEC 27035-2 — Information security incident management - Part 2: Guidelines to plan and prepare for incident response
33. ISO/IEC 27036-1 — Information security for supplier relationships - Part 1: Overview and concepts
34. ISO/IEC 27036-2 — Information security for supplier relationships - Part 2: Requirements
35. ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
36. ISO/IEC 27036-4 — Information security for supplier relationships - Part 4: Guidelines for security of cloud services
37. ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence
38. ISO/IEC 27038 — Specification for Digital redaction on Digital Documents
39. ISO/IEC 27039 — Intrusion prevention
40. ISO/IEC 27040 — Storage security[15]
41. ISO/IEC 27041 — Investigation assurance
42. ISO/IEC 27042 — Analyzing digital evidence
43. ISO/IEC 27043 — Incident investigation
44. ISO/IEC 27050-1 — Electronic discovery - Part 1: Overview and concepts
45. ISO/IEC 27050-2 — Electronic discovery - Part 2: Guidance for governance and management of electronic discovery
46. ISO 27799 — Information security management in health using ISO/IEC 27002 - guides health industry organizations on how to protect personal health information using ISO/IEC 27002.

ISO politics

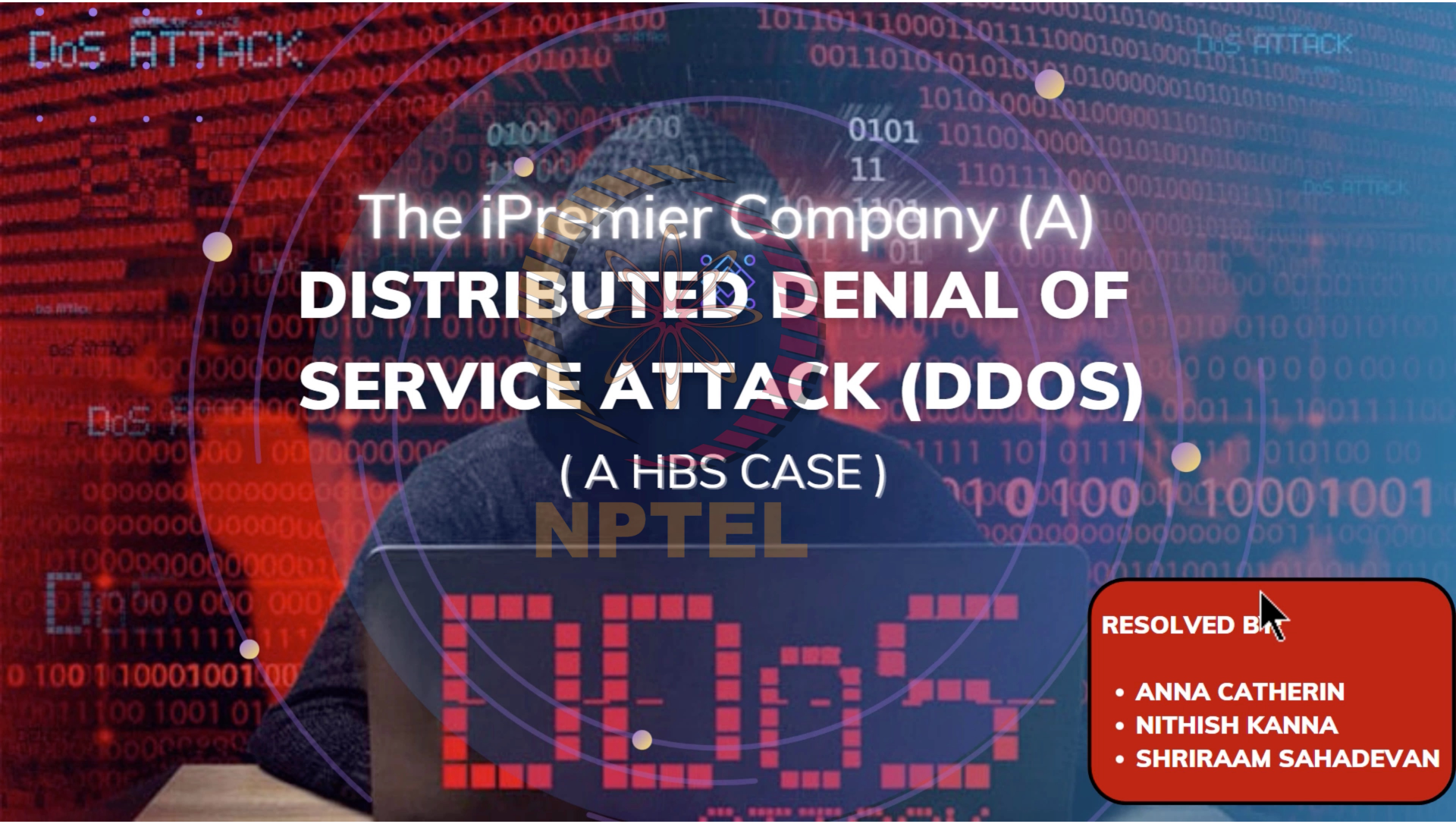
- Many countries, including the U.S., Germany, and Japan, have not adopted the model, claiming it is fundamentally flawed:
  - The global InfoSec community has not defined any justification for the code of practice identified
  - The model lacks "the necessary measurement precision of a technical standard"
  - There is no reason to believe the model is more useful than any other approach
  - It is not as complete as other frameworks
  - It is perceived as being hurriedly prepared, given the tremendous impact that its adoption could have on industry information security controls

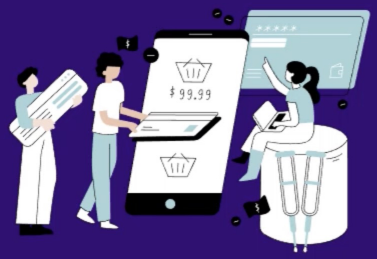
NIST security models

- NIST documents have two notable advantages:
  - They are publicly available at no charge
    - Open source vs proprietary debate
  - They have been available for some time and thus have been broadly reviewed by government and industry professionals
    - SP 800-12, Computer Security Handbook
    - SP 800-14, Generally Accepted Security Principles & Practices
    - SP 800-18, Guide for Developing Security Plans
    - SP 800-26, Security Self-Assessment Guide-IT Systems
    - SP 800-30, Risk Management for Information Technology Systems

SP 800-18: Guide for developing security plans

- The NIST Special Publication 800-18 offers an approach to policy management
- These policies are living documents that constantly change and grow
- These documents must be properly disseminated (distributed, read, understood, and agreed to) and managed
- Good management practices for policy development and maintenance make for a more resilient organization


DoS ATTACK
The iPremier Company (A)
DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)
(A HBS CASE)
NPTEL
RESOLVED BY
• ANNA CATHERIN
• NITHISH KANNA
• SHRIRAAM SAHADEVAN



iPremier Company

E-Commerce Business

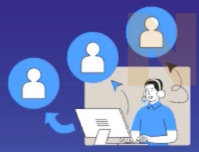
PRODUCTS

- Luxury,Rare and Vintage goods
- Prices range from Hundreds to Tens of Thousands of Dollars

COMPETITION

- iPremier one of top 2 websites
- Main competitor - MarketTop
- Competitive Edge - Best User Experience - attractive website,seamless service,after sales service etc

CLIENTS



- High end clientale
- Customer trust was crucial
- Over 1 million regular customers in database

MANAGEMENT CULTURE

- Mix of younger long term employees and experienced lateral hires
- Above average salaries - mainly as stock options
- Compensation linked to performance
- Intense environment - Qtrly reviews and removal of unsuccessful managers

Characters

Bob Turley,
CIO

Jack Samuelson,
CEO

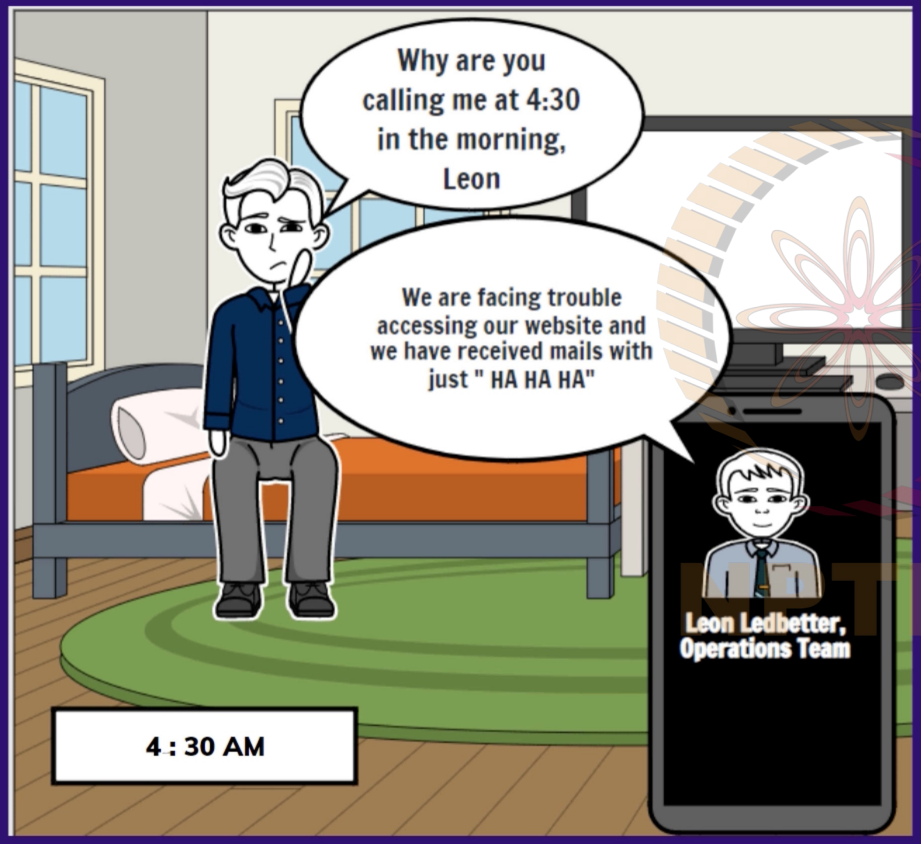
Tim Mandel
CTO,Cofounder

Warren
Spangler,
VP Business
Development

Peter Stewart ,
Legal Counsel

Joanne Ripley,
Operations
Team Leader

Leon Ledbetter,
Operations
Team

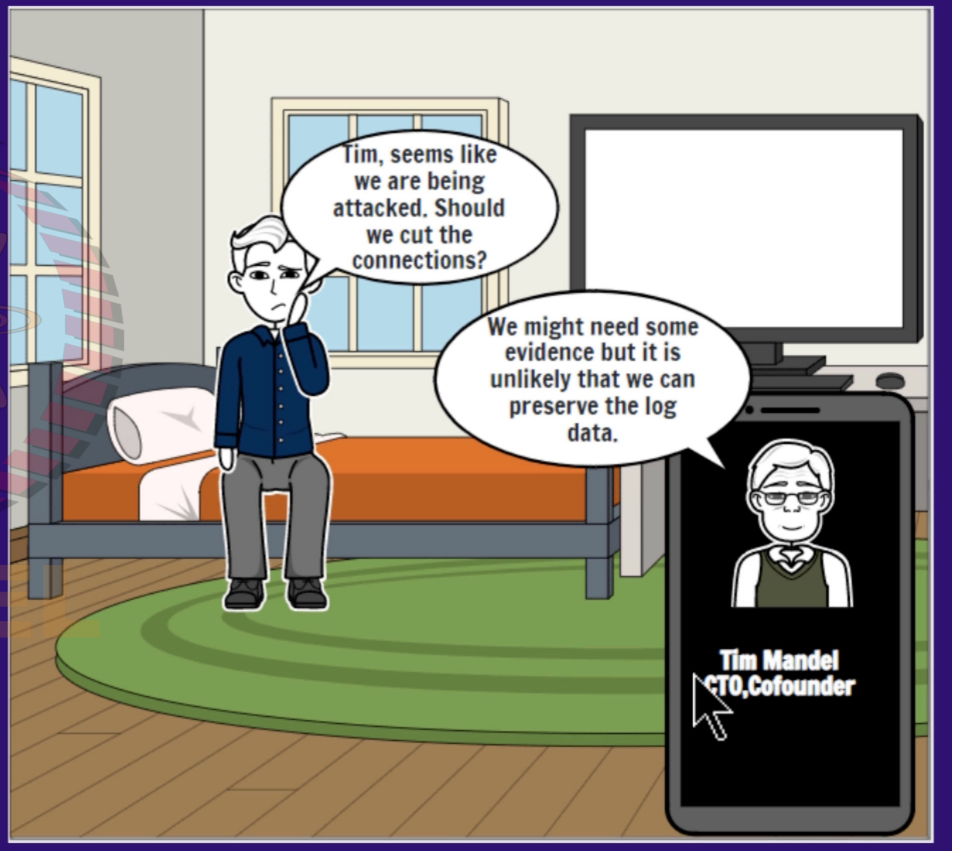

Why are you calling me at 4:30 in the morning, Leon
We are facing trouble accessing our website and we have received mails with just " HA HA HA"
Leon Ledbetter, Operations Team
4 : 30 AM

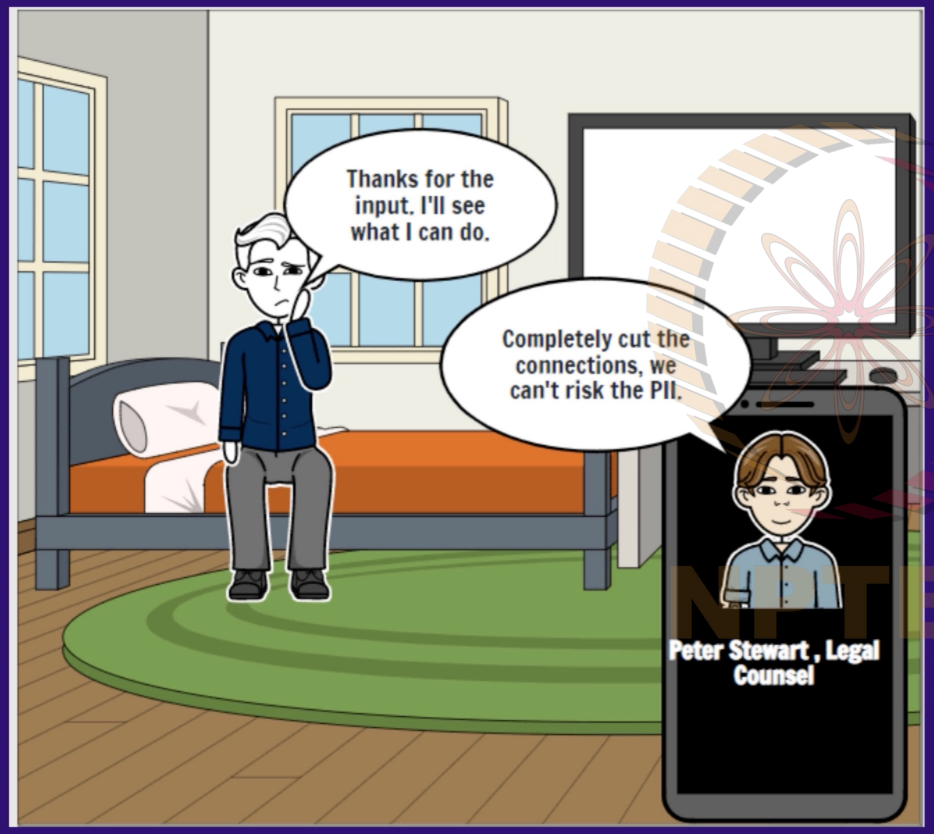

What's going on?
It doesn't look like a simple DDoS Attack
Joanne Ripley, Operations Team Leader
4:39 AM

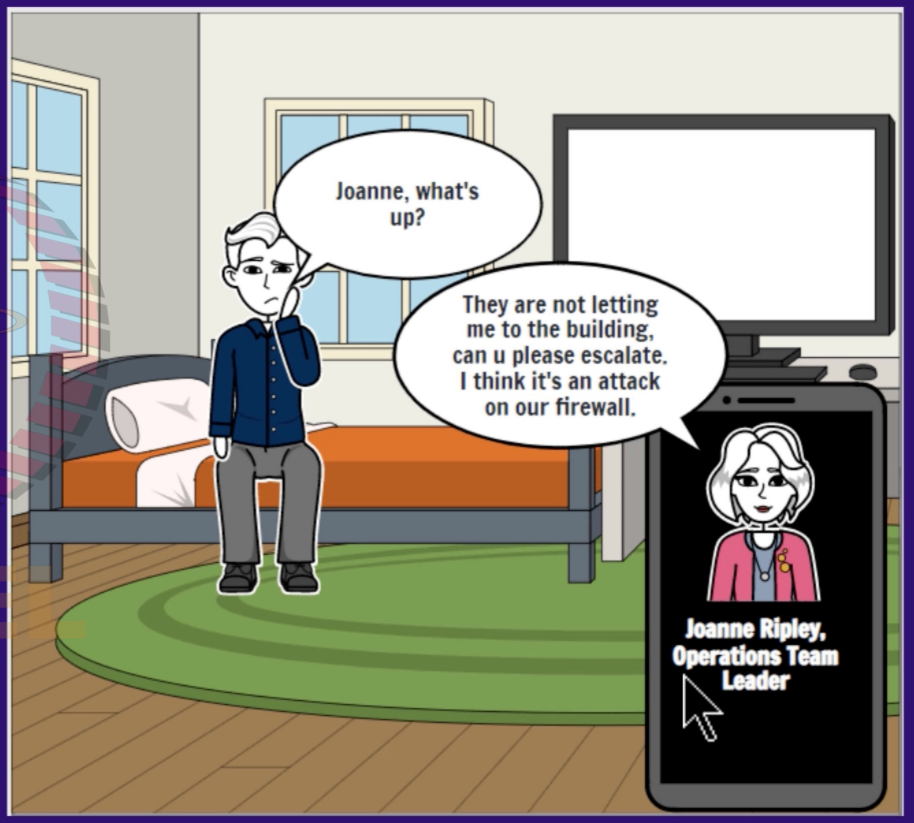

We are working on our solution
Stock will take a hit and I'll handle the PR
Warren Spangler, VP Business Development
4:43 AM


What are our emergency procedures?
We've got a BCP, but it's not been updated and we haven't practiced incident response
Joanne Ripley, Operations Team Leader

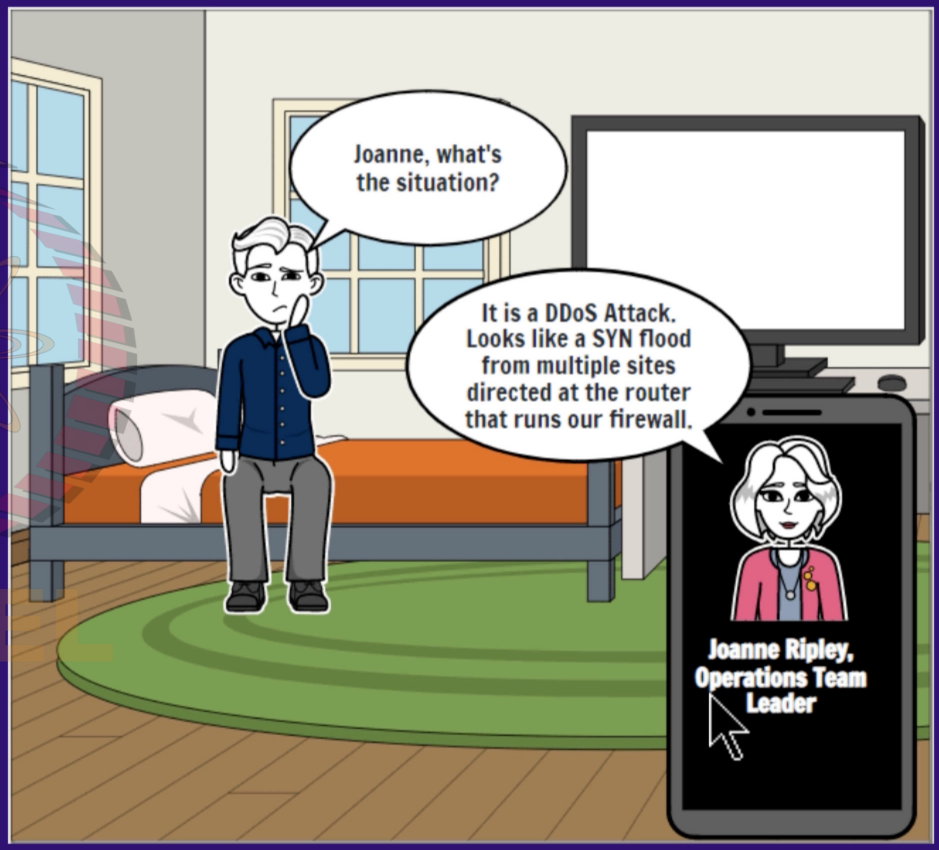

What are our options and are they stealing our data?
Let me go to QData and access the web server to see what's going on.
Joanne Ripley, Operations Team Leader


Tim, seems like we are being attacked. Should we cut the connections?
We might need some evidence but it is unlikely that we can preserve the log data.
Tim Mandel CTO,Cofounder


Thanks for the input. I'll see what I can do.
Completely cut the connections, we can't risk the PII.
Peter Stewart , Legal Counsel


Joanne, what's up?
They are not letting me to the building, can u please escalate. I think it's an attack on our firewall.
Joanne Ripley, Operations Team Leader


Not everything is going according to plan, but we are working a plan
Bob, the stock is probably going to be impacted and we'll have to put a solid PR face on this, but that's not your concern right now. You focus on getting us back up and running. Understand?
Jack Samuelson, CEO

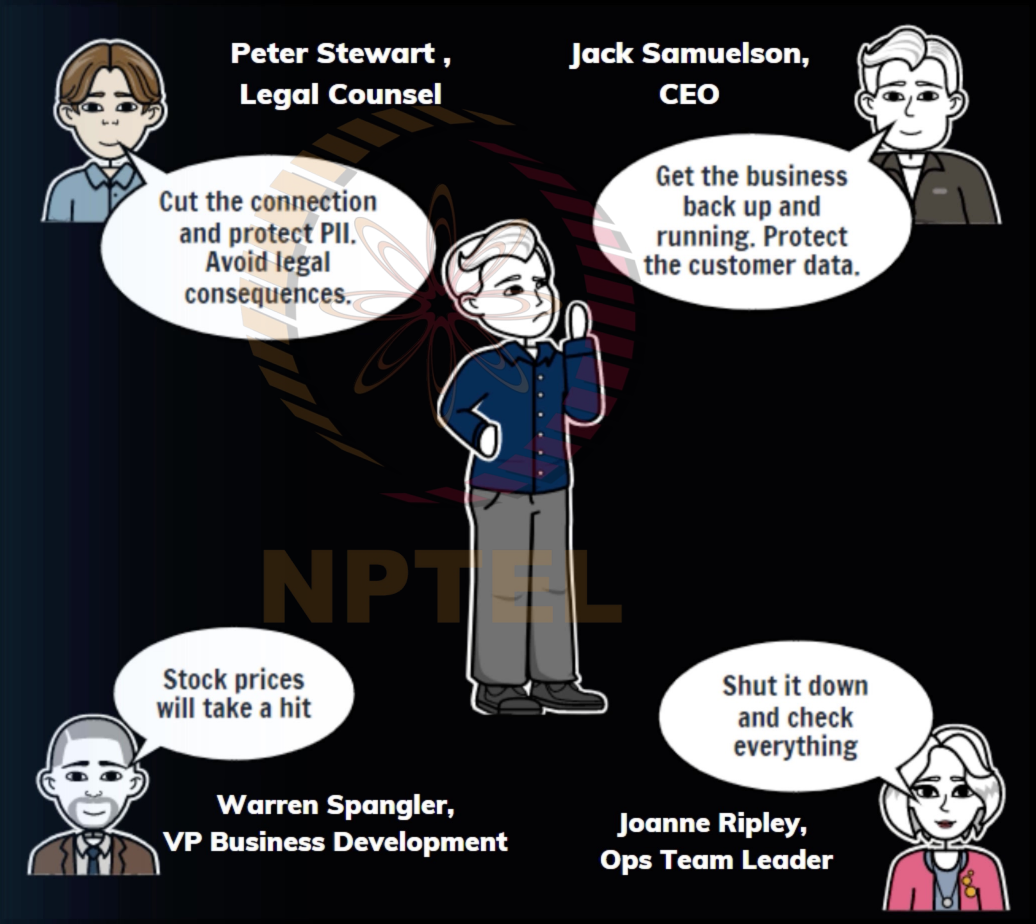

Joanne, what's the situation?
It is a DDoS Attack. Looks like a SYN flood from multiple sites directed at the router that runs our firewall.
Joanne Ripley, Operations Team Leader


What can we do right now? Is the customer data safe?
I can't cut the traffic as they are spawning zoombies. There is nothing that makes a DDoS attack and an intrusion mutually exclusive.
Joanne Ripley, Operations Team Leader


The attack stopped. It just stopped!!!
I didn't do anything.
Joanne Ripley, Operations Team Leader


What now? Is it business as usual?
The website is running. We can resume the business as usual. But I recommend we shut down
Joanne Ripley, Operations Team Leader

Stakeholders Perspective



Distributed Denial of Service

DDoS stands for distributed denial of service and is often used to reference a type of network attack and these attacks are subclass of regular denial-of-service (DoS) attacks.

Attack attempts to overwhelm an Internet-connected asset with the aim of making it unavailable to legitimate users.

DoS vs. DDos Attacks

DoS Attacks

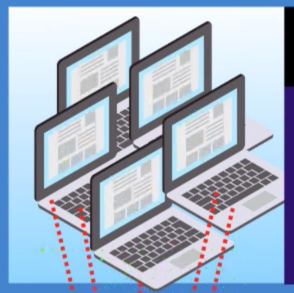
- Use single-sourced devices
- Create fake traffic
- Exhaust server resources
- Occur on a smaller scale

DDoS Attacks

- Use botnets
- Manipulate real traffic
- Overwhelm a network with traffic requests
- Occur on a larger scale

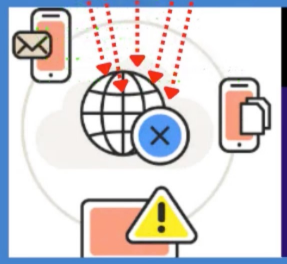
ATTACKER

A hacker infects devices to make botnets, forming a zombie network



ZOMBIE NETWORK

The zombie network floods a targeted website or server with traffic



TARGETED WEBSITE/SERVER

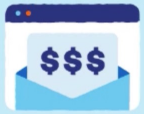
Targeted website or server crashes, disconnecting from the internet

DDoS Attack Motives

HACKTIVISM

CYBERVANDALISM

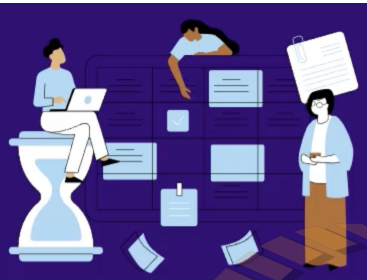
CYBERWARFARE



EXTORTION

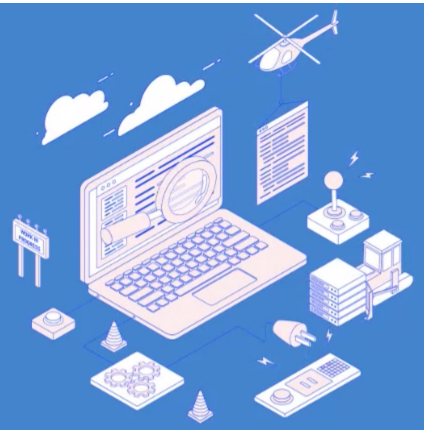
RIVALRIES


What
went
wrong?



Managerial

- Lack of a tested and updated business continuity plan
- Inadequate training for emergencies
- Lack of security and risk expert
- Develop a better relationship with your hosting provider
- Lack of independent audit team who report into the board
- Make security part of strategy



Technical

- Lack of proper firewall
- iPremier did not use detailed logging software that might give them evidence of what was going wrong during the attack and who attacked them

Immediate Course of Action

- Shutting down to conduct a thorough forensic audit

Reasons :

- *Understand more about the nature of attack*
- *Identify the vulnerabilities in the system*
- *To safeguard from future cyberattacks*

Immediate Course of Action

- Shutting down to conduct a thorough forensic audit

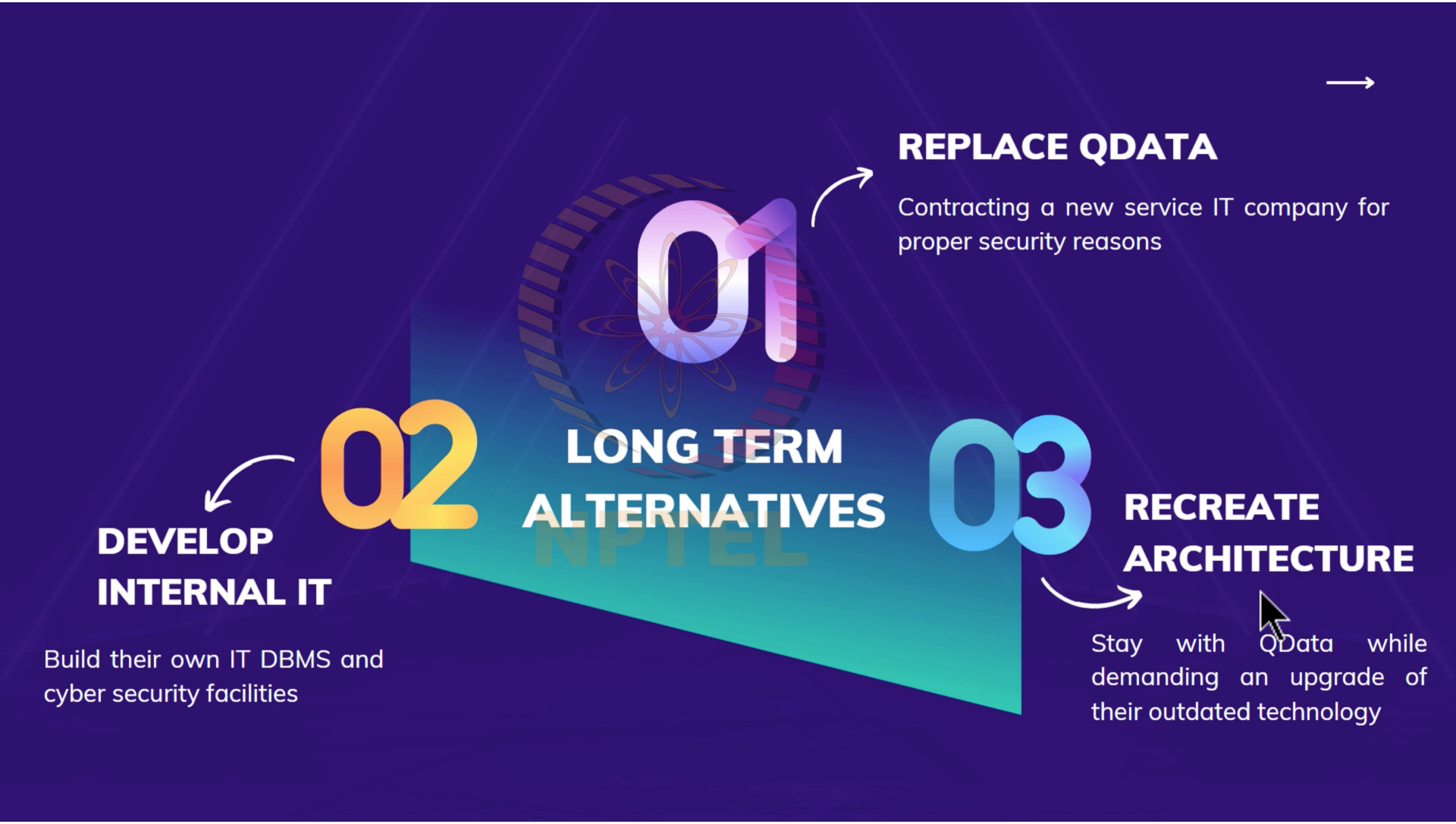
Reasons :

- *Understand more about the nature of attack*
- *Identify the vulnerabilities in the system*
- *To safeguard from future cyberattacks*

- Deal with the PR team
- Issue a statement stating a temporary server downtime owing to unexpected high traffic while giving customer privacy the highest priority

Reasons :

- Be responsible for what had happened
- Hiding might make us more vulnerable to hackers as well as competitors


01
REPLACE QDATA
Contracting a new service IT company for proper security reasons
02
DEVELOP INTERNAL IT
Build their own IT DBMS and cyber security facilities
LONG TERM ALTERNATIVES
03
RECREATE ARCHITECTURE
Stay with QData while demanding an upgrade of their outdated technology

01 REPLACING QDATA WITH A BETTER SERVICE PROVIDER

Contracting / Outsouring to top internet service providers and DBMS for better services

PROS	CONS
State-of-the-art infrastructure	Increased spend on financial resources
Improved defense mechanism with constant updates and patches	Time Consuming Process
Increased Customer Trust	Affects personal commitment with owner QData

02 DEVELOP INTERNAL IT SYSTEM

Build their own IT DBMS and cyber security facilities

PROS	CONS
+ Full control over their database system	− Costly affair
+ Cost-effective in the long run	− TIme Consuming
	− Outcome is not guaranteed

03 STAY WITH QDATA WHILE RECREATING THE ARCHITECTURE

Resume with Qdata but demand investing on newer technology and ensure a proper workflow

PROS	CONS
+ Helps avoid switching costs for iPremier	− Revised contract terms and prices
+ Saves time in returing to normalcy compared to switching	− Updating might take significant time
+ Long term relationship is restored	