Mainframes, Ransomware and PCI Requirements

Allen Saurette, Thought Leader
MainTegrity, Inc

The facts

A cyber attack occurs

every **39** sec

Source: Security Magazine

Verizon

34%

Involved internal actors

Verizon

32%

of breaches Involved phishing

Accenture

$13M

Avg cost of Cybercrime for an organization

Share.org

90%

of Credit transactions go through a mainframe

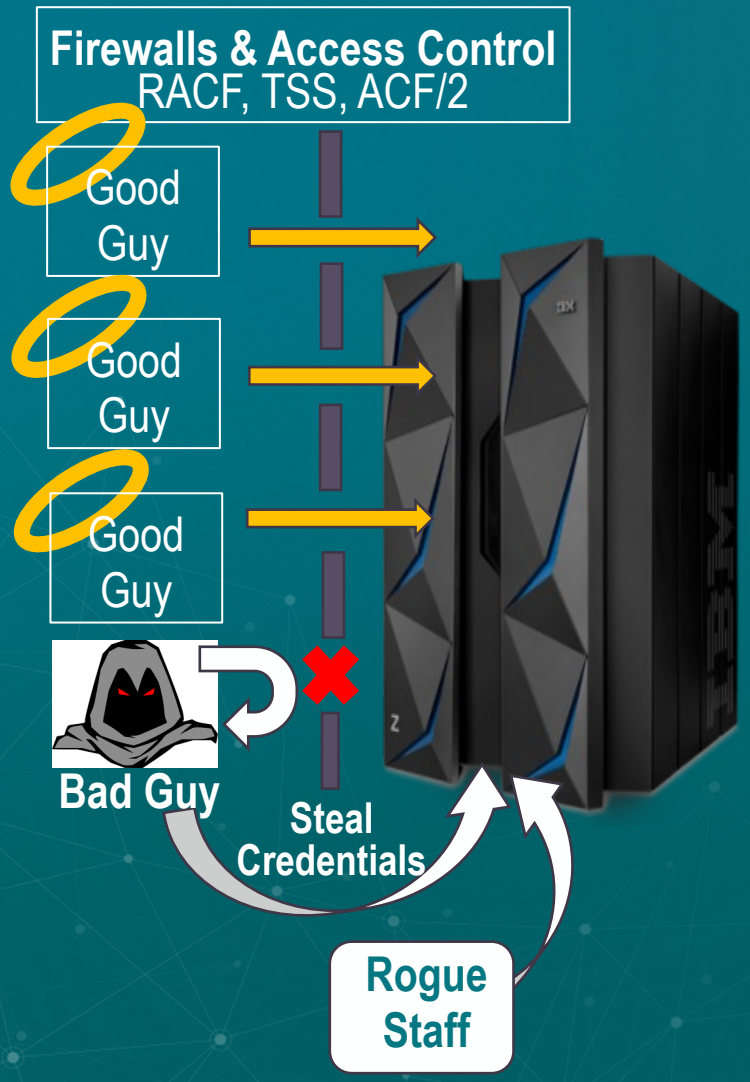
Avg. cost of cyber attack

(Accenture)

Industry	Avg Cost
Banking	$18.4M
Utilities	$17.8M
Software	$16M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

Courtesy of DELL Technologies

Conventional Security



Guard the perimeter

- Insiders are past Firewall / Access Control
  1. Bad Guys Steal / Buy Credentials on dark web
  2. Trusted employees go rogue (addiction, financial, health)

Detect attacks other tools miss

- Changes look legitimate, so hard to detect
- Pen Testers often find dozens of gaps
- Attacks missed in mainframe logs and security tools

No matter how good your perimeter defences are motivated criminals will get access

PCI DSS V3.2.1 & FIM

Required on all computers handling Debit / Credit

Sec 10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?

Sec 11.5	Is a change-detection mechanism (for example, **file-integrity monitoring tools**) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files?

PCI Security Standards Council

Section 3: …..Part 3. PCI DSS Validation

☑ **Compliant:** All sections of PCI DSS complete, all questions answered affirmatively

Part 3b. Attestation

Signature of Executive Officer _____

Executive Officer Name: _____ *Date:*

Title: Your CIO, Your CFO, Your CEO

Integrity Monitoring

Detect & Recover from cyber intrusion

- Create baseline at trusted state
- Store keys in an encrypted vault
- Learn routine changes when deployed
- Subsequent scans detect / alert on unauthorized changes
- Forensics browser gathers logs, integrity and other relevant security data
- Restores data from with immutable and conventional backups
- Surgical restore for **software infrastructure**

Old Attacks

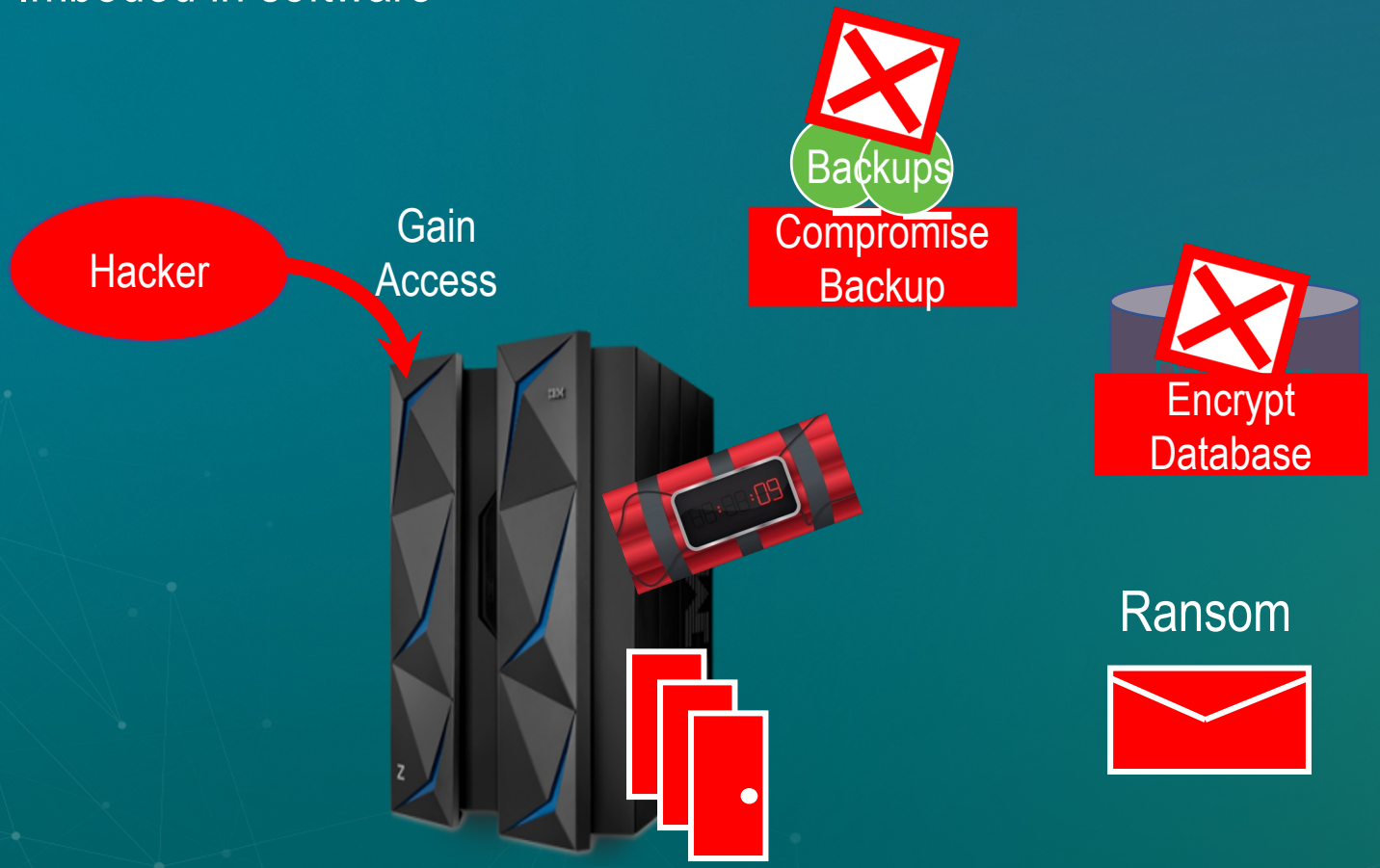
Sport or Spite, not for Profit

Break in:

1. Gain Access
2. Attack Database
3. Recover Data

Ransomware – new threats

Malware – Imbeded in software

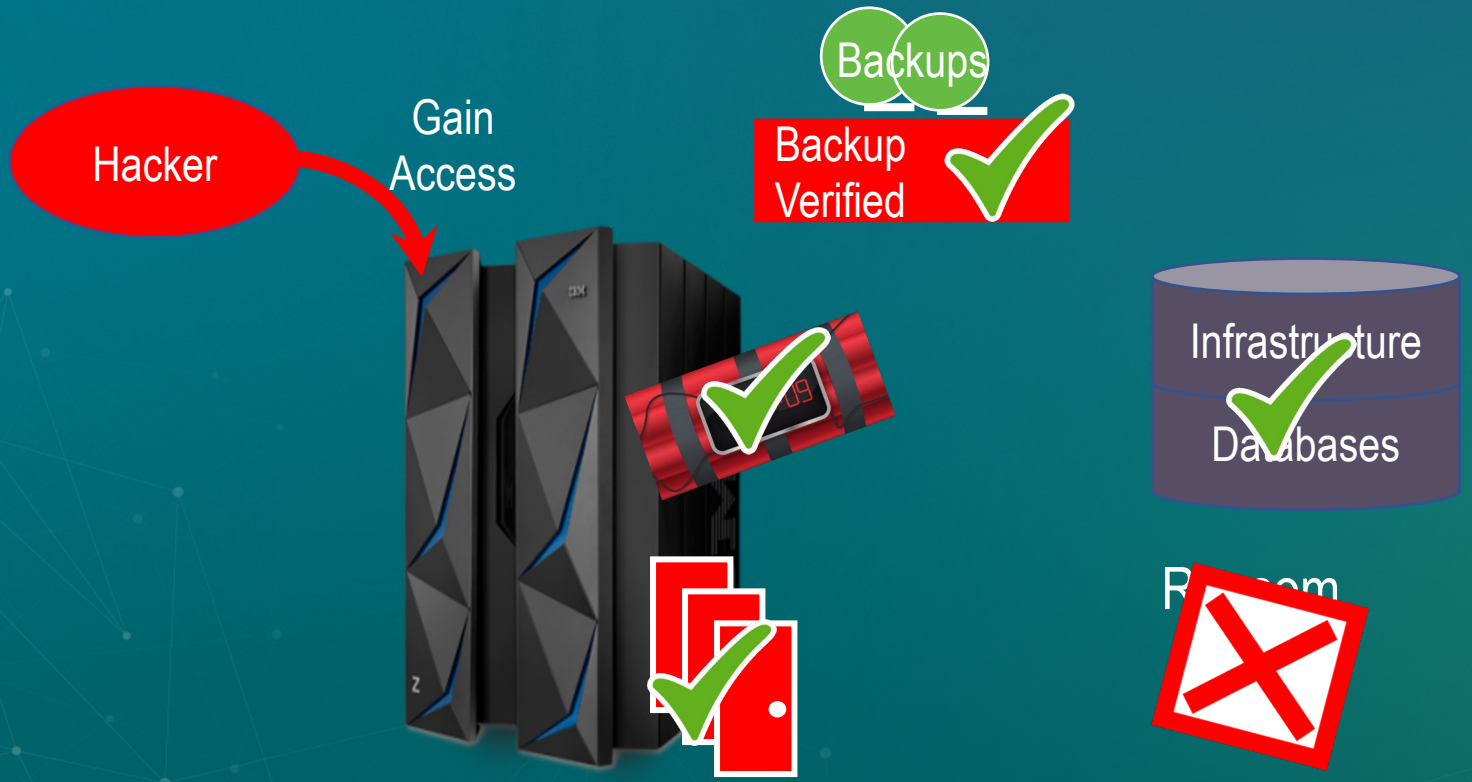


Attacking as a business

- Persistent, intelligent
- Multiple Backdoors
- Timebombs
- Compromise Backups
- Attack Database
- Ransom Demand

Ransomware Resolved

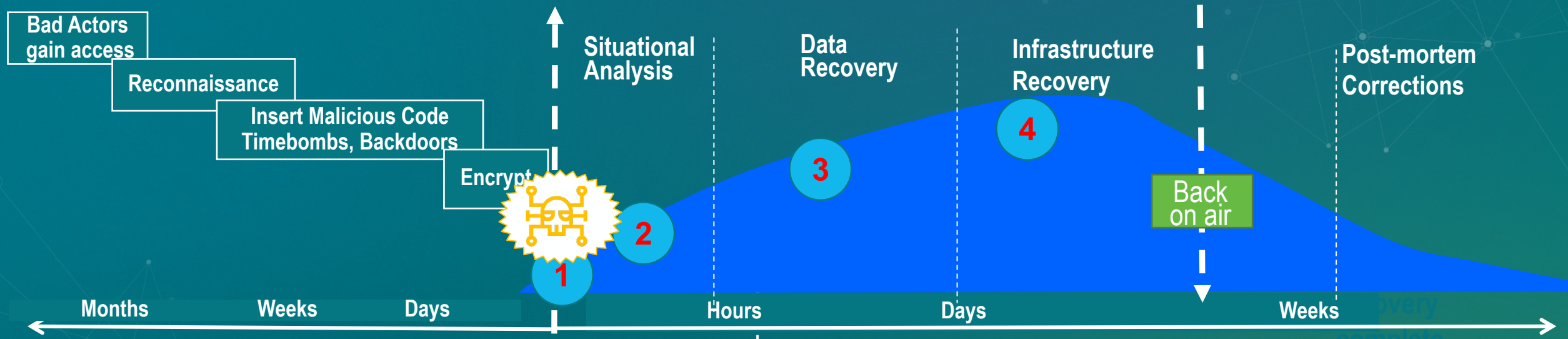
Restore data & infrastructure – without regression



What is needed?

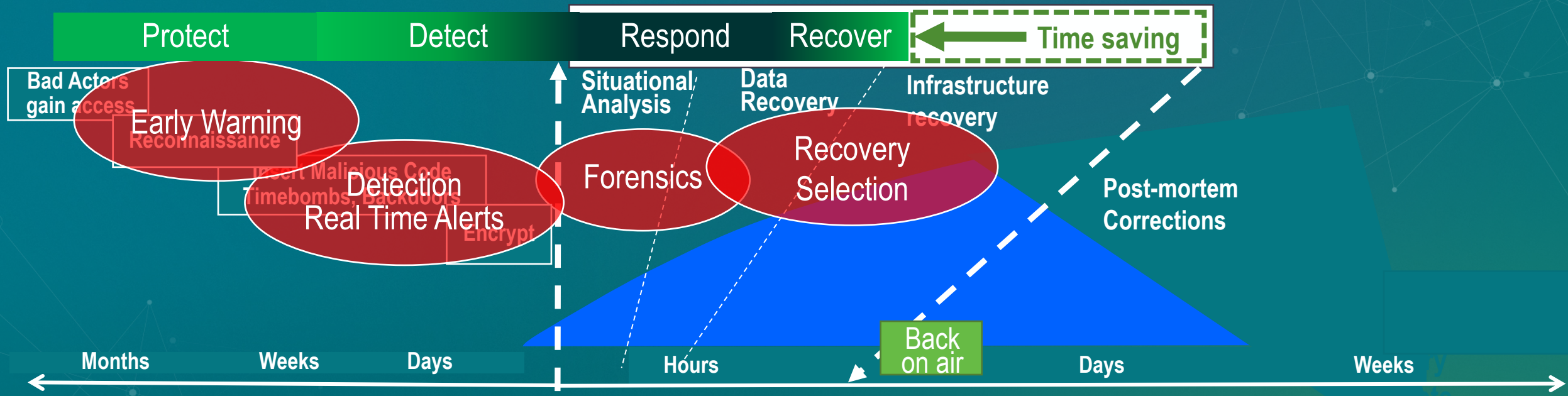
- Early attack detection
- Scope – see malicious mods
- Verified Backups / Logs
- Fast reaction – Forensics
- Infrastructure & Data Restore
- Prevented paying ransom

Typical Attack Recovery



1. Corruption of data occurs
2. Try to determine - what was affected, when
3. Find best source for data recovery
4. Review all changes - hope to find malicious ones

Fast Data & Software restore



Integrity Monitors tools can:

Forensics - know what is affected, when correct, who

Verify Backups uncompromised

Recover Infrastructure & data - no regression

Detect first malicious changes - alert

Early Warning – Flag suspicious acts, prevent attack

Public Example

As reported by CBC News Oct 7, 2018
17 federal departments and agencies have flunked a basic test of their credit card data security."
failures

Those 17 departments and agencies continue to process payments on Visa, MasterCard, Amex …

- To our knowledge no remediation implemented (in 5 years)
- Specifically, no steps to comply with sections 10.5 and 11.5
- How many PCI Audits have highlighted these problems?

Session takeaways

- Mainframes are not immune to internal threats
- Integrity Monitoring compliments existing security tools
- Ransomware can be beaten - PCI DSS controls help
- Joint Responsibility:
  - Software suppliers - create superior security solutions
  - Customers – implement proper security
  - People in this room – Enforce the controls

Mainframes are high value targets – protect them well

Allen Saurette, Al@MainTegrity.com, 403 818-8625