Oracle Database Security Master Class

Slide Deck 1

Daniel A. Morgan
email: damorgan@dbsecworx.com
mobile: +1 612-240-3538

09 May 2019

Unsafe Harbor Statement

- This room is an unsafe harbor
- You can rely on the information in this presentation to help you protect your data, your databases, your organization, and your career
- No one from Oracle has previewed this presentation
- No one from Oracle knows what I am going to say
- No one from Oracle has supplied any of my materials
- Everything I present is existing, proven, functionality

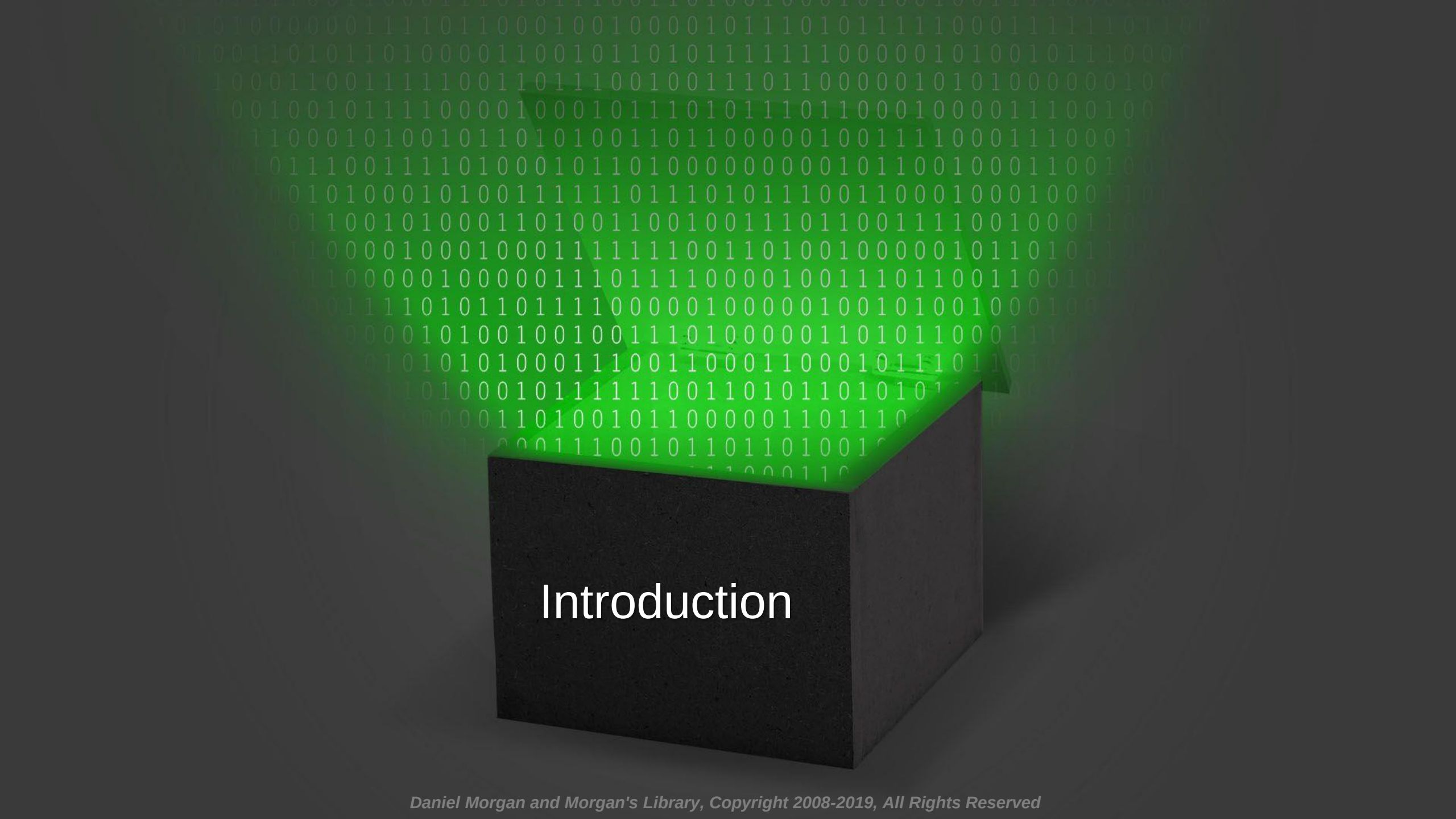
This Week

The Cybersecurity Industry Makes Millions, But Is It Keeping Us Safe?

The cybersecurity industry is booming. As thousands meet at the RSA security conference, it's fair to wonder: What are all these companies actually doing?

SHARE TWEET

Last year, investors poured $5 billion in cybersecurity startups. The whole industry will be worth $170 billion in three years, according to a recent estimate. There's so many infosec companies that it's becoming difficult to keep track of them all. And yet, are we all any more secure? Is the infosec industry really keeping us safe? Is it even focusing on the right problems?



Introduction

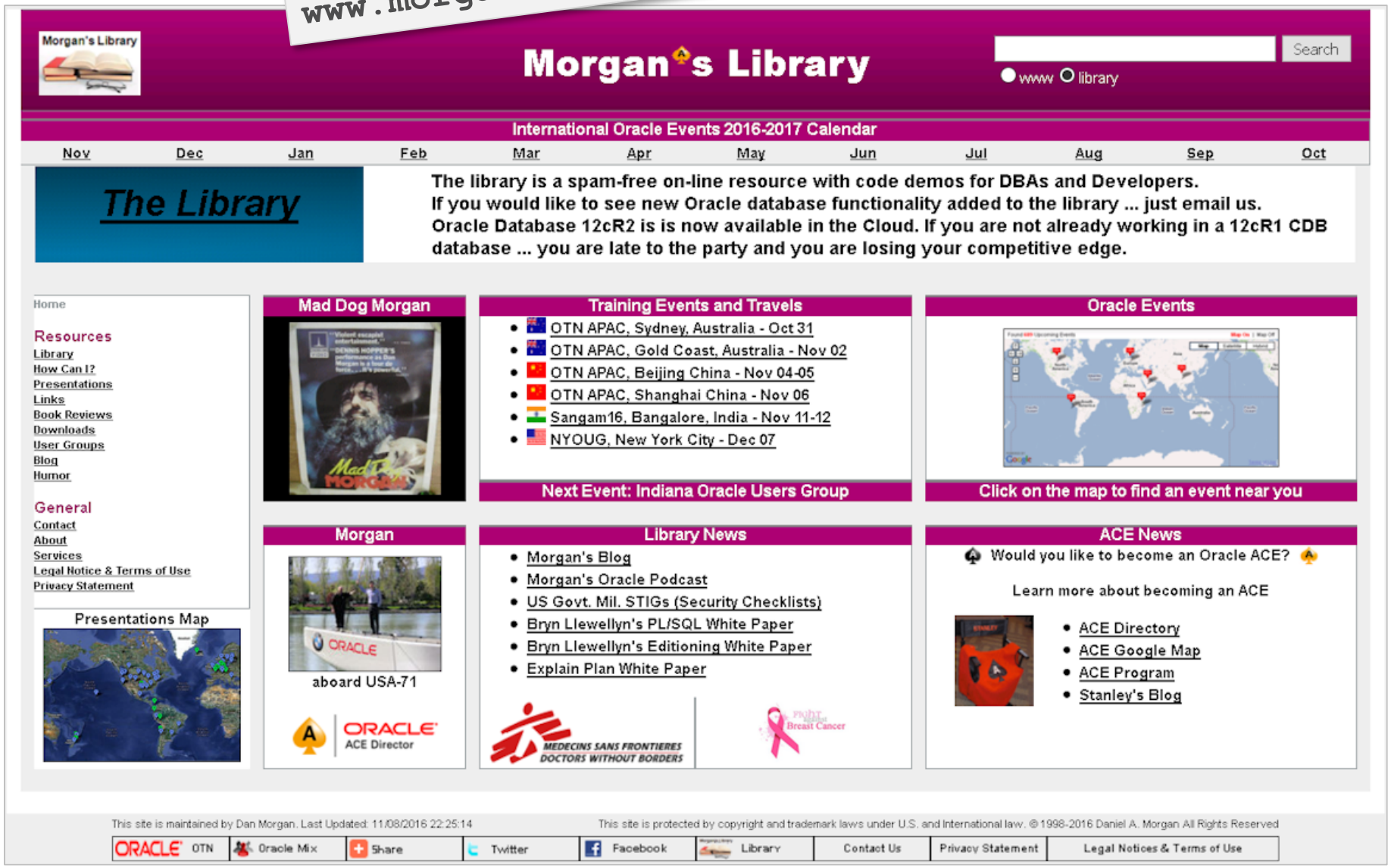
Daniel A. Morgan

- Managing Director: Database Security Worx
- Oracle ACE Director Alumni
- Oracle Educator
  - Adjunct Professor, University of Washington, Oracle Program, 1998-2009
  - Consultant: Harvard University
    - Guest lecturer at universities in Canada, Chile, Costa Rica, New Zealand, Norway, Panama
    - Frequent lecturer at Oracle conferences … 132 countries (42 unique) since 2008
- IT Professional
  - Celebrating 50 years of IT in 2019
  - First computer: IBM 360/40 in 1969: Fortran IV
  - Oracle Database and Beta Tester since 1988-9
  - The Morgan behind www.morganslibrary.org
  - Member Oracle Data Integration Solutions Partner Advisory Council
  - Member Board of Directors, Northern California Oracle Uses Group
- damorgan@dbsecworx.com

System/370-145 system console

My Personal Website ... (zero advertising, zero tracking)

www.morganslibrary.org



Forbes Magazine 2018

ForbesBrandVoice® What is this?

JAN 15, 2018 @ 05:00 AM 20,020

3 Essential DBA Career Priorities For 2018

OracleVoice

Simplify IT, Drive Innovation FULL BIO

Jeff Erickson, Oracle

Many database administrators (DBAs) will go into 2018 wondering if "self-driving" databases will weaken their career prospects. More likely, 2018 will be a year that database technology leaps forward and these valuable data experts take on other, more important responsibilities.

"History is repeating itself," says longtime DBA Dan Morgan, founder of Morgan's Library and principal adviser at tech firm Meta7. Morgan has seen the DBA role evolve amid a long series of technical advances in storage, management, and performance. And each advance asked DBAs to adjust the way they work.

Travel Log: Chile 2010

Travel Log: Galapagos Islands, Ecuador 2014

Auditing

- What is auditing

> A **security audit** is a systematic evaluation of the **security** of a company's information system by measuring how well it conforms to a set of established criteria.

> A supplement to the **FAR** that provides DoD-specific acquisition regulations that DoD government acquisition officials – and those contractors doing business with DoD – must follow in the procurement process for goods and services. **DFARS** – Defense Federal Acquisition Regulation Supplement

- What does auditing not do?
  - Consider the first definition ... "conforms to a set of established criteria"
- Were the audit criteria created by a Subject Matter Expert?
- In what subject?
- Were they written by people with expertise breaking into databases?
- When was the last time the criteria were updated to reflect a new vulnerability?

Compliance

- What is compliance

A **compliance audit** is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of **compliance** preparations.

- What does a compliance audit not accomplish?
- Who defined the compliance criteria?
- What is the expertise of those verifying complia
- What is the expertise of those rating and rankin
- Do those performing the compliance audit have outcome?
- What mechanism enforces follow-up actions?

Governance

- What is governance

> **Corporate governance** is the system of rules, practices and processes by which a firm is directed and controlled. Corporate governance essentially involves balancing the interests of a company's many stakeholders, such as shareholders, management, customers, suppliers, financiers, government and the community.

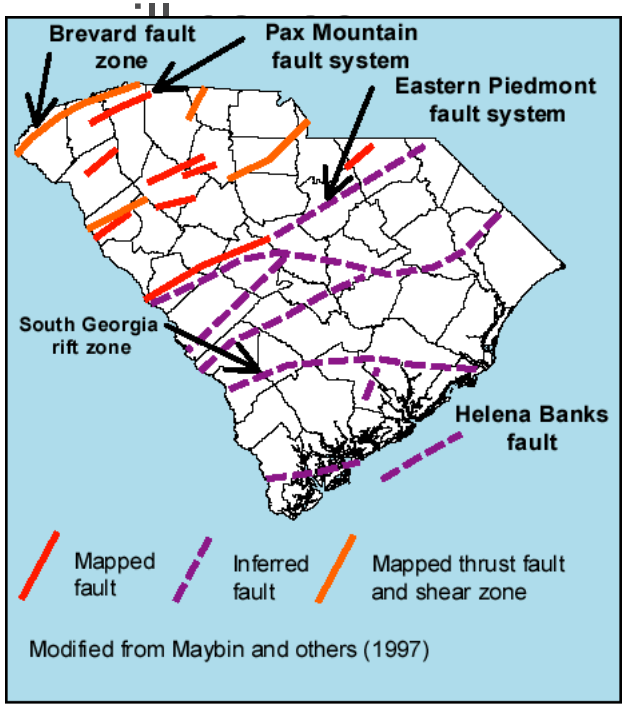
- Who establishes the rules, practices, and processes?
- Do those establishing them fully understand the risks and rewards they are balancing?
- The chance of an asteroid hitting Everett Washington is very small ... but not zero ... we cannot stop one today or tomorrow so we don't need to write rules
- The chance of Boeing data being found in Beijing, Moscow, Pyongyang, or Tehran is very high ... and we can absolutely do something to either prevent it or minimize the risk

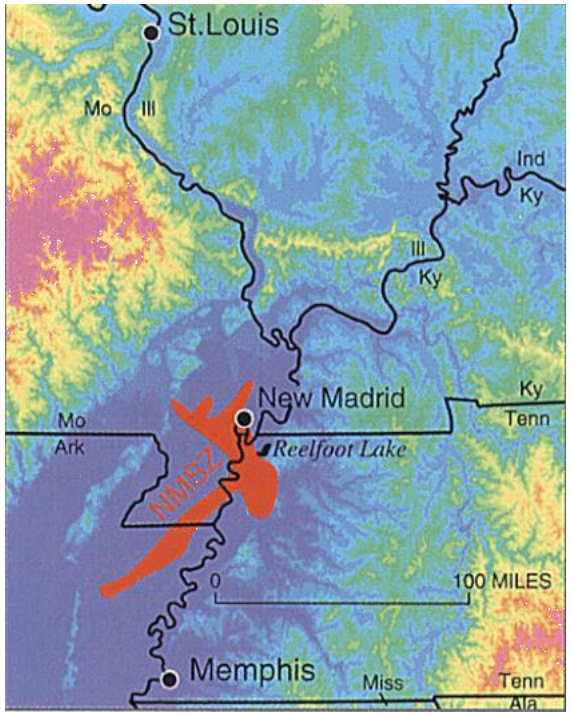
Mitigation

- What is mitigation

> A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence. Also called risk reduction.

- There are risks we cannot eliminate
- We cannot eliminate earthquakes ... but we can minimize the damage they





Security

- What is security

> Data **security** refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type.
> Data security is also known as **information security (IS)** or computer security.

- Is there any point of intersection between this definition and the ones we just reviewed?
- Only one ... the same intersection that exists after someone breaks into your house, steals everything you own, gets your passport, your social security card, and uses them to clean out your bank and investment accounts
- Auditing, after the damage is already done, tells you what you wouldn't have lost if you had focused on better security

Terminology

- Attack Surface
  - Any node on the network that can be attacked. It can be the UI, People, anything or anybody that accesses data
- Exploit
  - Take advantage of a flaw or feature
- Hack
  - Anything that can be hacked
  - Do something it was not intended to do or something you did not think it could do
- Leak
  - Sensitive data has spilled outside of it's protected environment. It has been compromised
- Perimeter
  - Placing safeguards at the entrance points to a network: A firewall
- Spillage
  - Sensitive data has "spilled" outside it's protected environment. It may not have been compromised

American Lack of Attention to Details

STORING PASSWORDS LIKE IT'S 1999 —

Plain wrong: Millions of utility customers' passwords stored in plain text

"It's ridiculous vendors are replying to researchers via general counsel, not bug bounty."

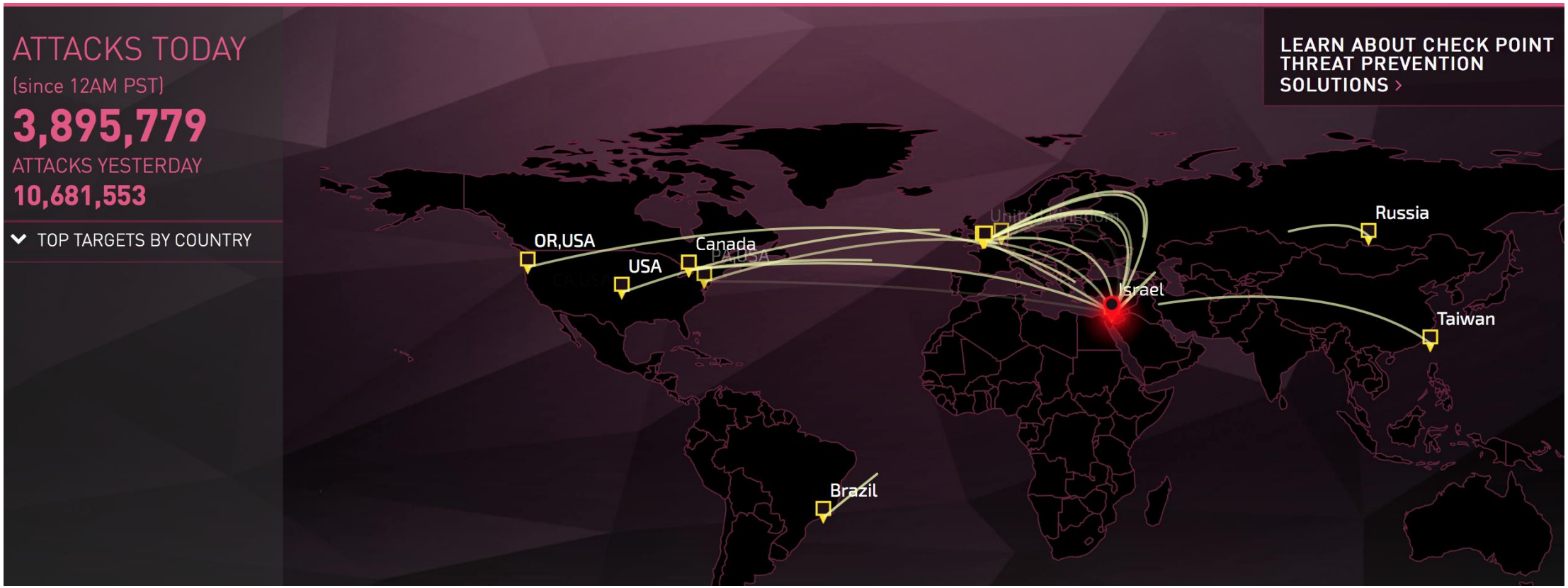
JIM SALTER - 2/25/2019, 6:30 AM

137

In September of 2018, an anonymous independent security researcher (who we'll call X) noticed that their power company's website was offering to email—not reset!—lost account passwords to forgetful users. Startled, X fed the online form the utility account number and the last four phone number digits it was asking for. Sure enough, a few minutes later the account password, in plain text, was sitting in X's inbox.

This was frustrating and insecure, and it shouldn't have happened at all in 2018. But this turned out to be a flaw common to websites designed by the Atlanta firm SEDC. After finding SEDC's copyright notices in the footer of the local utility company's website, X began looking for more customer-facing sites designed by SEDC. X found and confirmed SEDC's footer—and the same offer to email plain-text passwords—in more than 80 utility company websites.

The Threat Map (1:2)



`https://threatmap.checkpoint.com/ThreatPortal/livemap.html`

The Threat Map (2:2)

- What you are looking at is both real and real-time
- This is not the work of a bunch of bored teenagers and script kiddies
- This is the work of dedicated IT professionals
- 99+% of it comes from one of two sources

- Organized crime organizations ... if they gain access your data will be sold on the dark web or used to create or control bank or credit card accounts

- Nation-States ... if they gain access your data will be used to attack our country, our economy, your community, your employer and your family

- This is NOT hyperbole ... this is reality

Database Risks

- Most databases break-ins are never detected, never reported
- What you hear about is the part of the iceberg above the water
- Database related risks fall into three broad categories
  - Data Theft
  - Data Alteration
  - Transforming the database into an attack tool
- To accomplish these activities requires gaining access and doing so generally falls into one of the following categories
  - Utilizing granted privileges and privilege escalation
  - Access to Oracle built-in packages
  - SQL Injection

Oracle Management & Security Cloud (1:2)

Oracle Management & Security Cloud (2:2)

We Cannot Win By Buying Products ... We Must Change The Rules

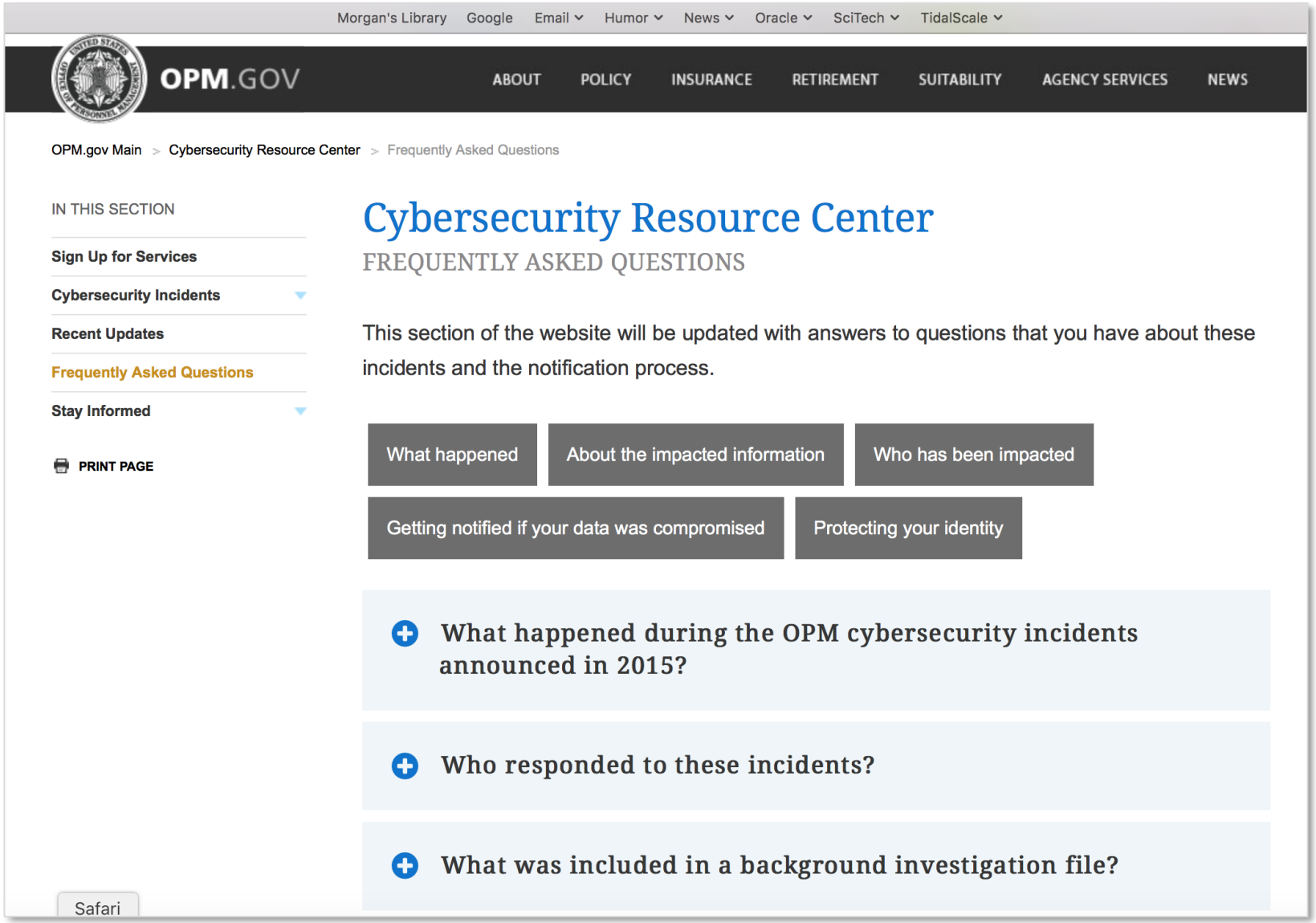
- Our databases and data are not being attacked fingers on keyboards
- The attackers do not come to work between 8am and 5pm Monday - Friday
- They don't get called into meetings
- Their phone doesn't ring
- They don't go out to lunch
- They don't go home after work
- They don't take off weekends and holidays
- They don't get sick leave
- They don't go on vacation
- They are bots

- If we fight this war as humans vs bots we will always lose

We Can Only Win The War If We Fight As Equals

Anyone want to play chess against Deep Blue?
Anyone rational person think they can beat AlphaGo?

Office of Program Management (1:5)



Office of Program Management (2:5)

What happened during the OPM cybersecurity incidents announced in 2015?

In 2015, OPM announced malicious cyber activity on its network and identified **two separate but related cybersecurity incidents** that have impacted the data of Federal government employees, contractors, and others. First, OPM discovered malicious cyber activity on its network resulting in the exposure of the personnel data of approximately 4.2 million current and former Federal government employees. Second, OPM discovered malicious cyber activity on its network resulting in the exposure of the background investigation records of approximately 21.5 million individuals, primarily current, former, and prospective Federal employees and contractors.

Office of Program Management (3:5)

- Did OPM have governance requirements?
- Did OPM have regulatory requirements?
- Did OPM pass its compliance audits?
- Did OPM meet or exceed NIST requirements?
- Did OPM hire qualified security professionals?
- Did OPM hire qualified network, storage, system, and database admins?
- Did OPM have a firewall?
- Did OPM monitor network activity?
- Did OPM patch its firmware and software?
- Did OPM use userids, passwords, and multi-factor authentication?

But none of this has anything to do with data and database security

Office of Program Management (4:5)

- OPM pretends the breach perpetrated by the People's Republic of China was for purposes of obtaining credit cards

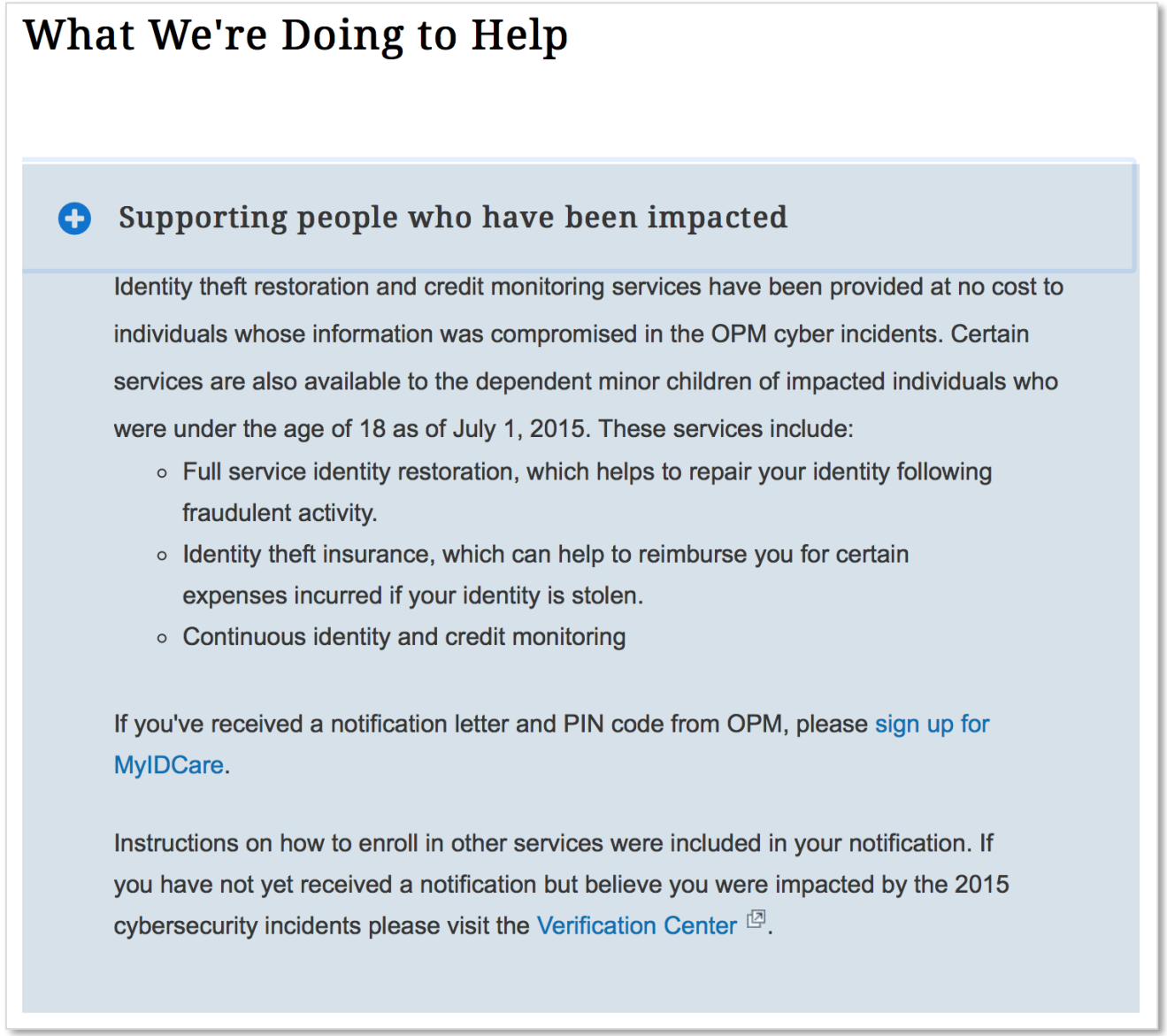
  seriously ... they offered all of us whose data was taken free credit reports

  what did they think the People's Liberation Army was going to do with my DOB and SSN?

  go shopping at Nordstrom's?
  get a stereo system at Best Buy?
  get an AmEx card?

Office of Program Management (5:5)

- Perhaps I like to live dangerously but for some reason I didn't consider it likely the PRC would be selling my finger prints, photographs, and family history to identity thieves
- So I didn't sign up and volunteer to a credit bureau that I has applied for a security clearance
- Thus further compromising what was left of my identity



What We're Doing to Help

Supporting people who have been impacted

Identity theft restoration and credit monitoring services have been provided at no cost to individuals whose information was compromised in the OPM cyber incidents. Certain services are also available to the dependent minor children of impacted individuals who were under the age of 18 as of July 1, 2015. These services include:

- Full service identity restoration, which helps to repair your identity following fraudulent activity.
- Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
- Continuous identity and credit monitoring

If you've received a notification letter and PIN code from OPM, please sign up for MyIDCare.

Instructions on how to enroll in other services were included in your notification. If you have not yet received a notification but believe you were impacted by the 2015 cybersecurity incidents please visit the Verification Center.

Anatomy Of Reality

- I am going to tell you about a breach that has never been publicly revealed
- It happened within the last 3 years
- It happened in the United States
- And you will not find a single reference to it with the google search engine

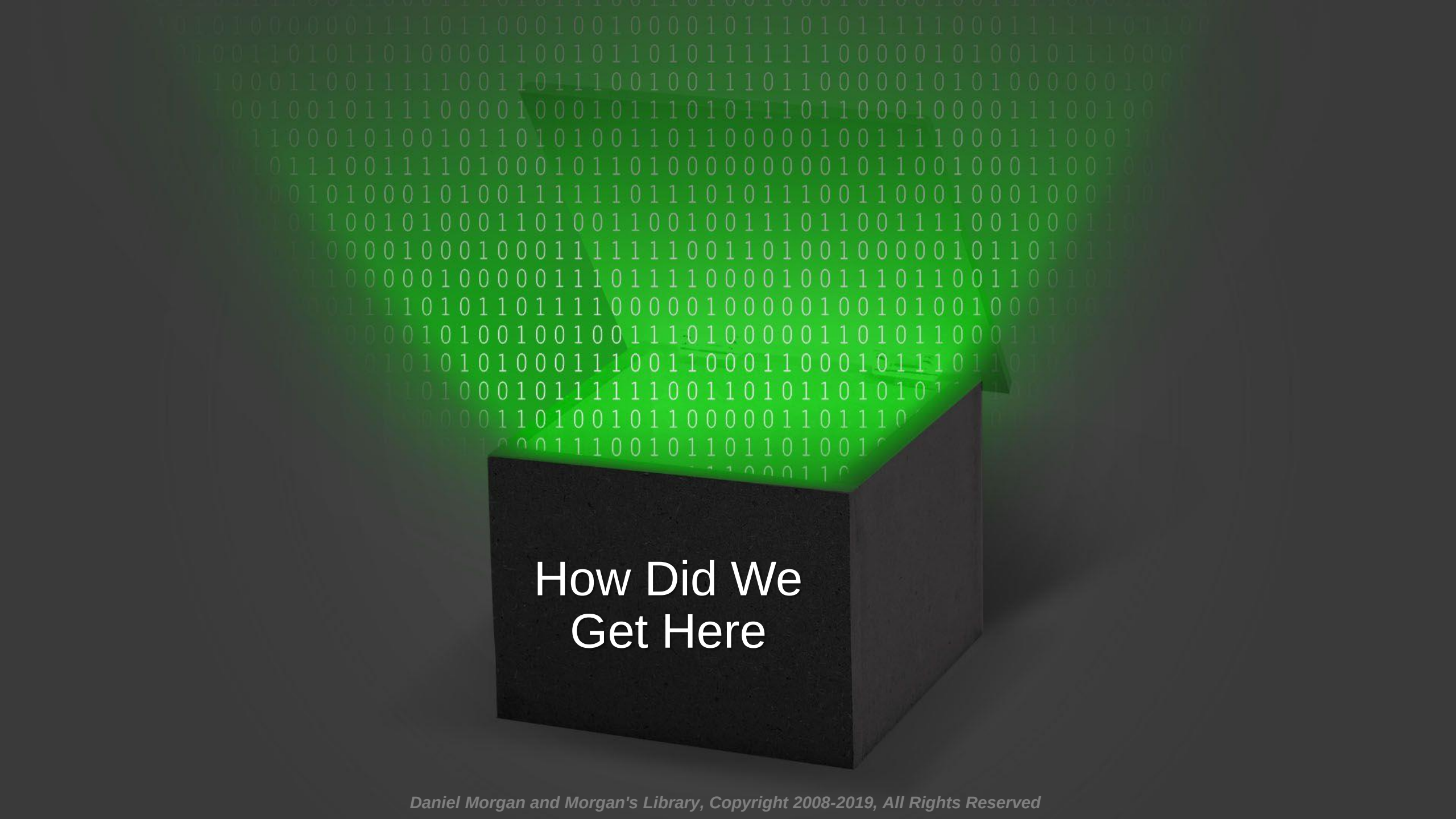
An Unpleasant Fact

- Governance is NOT security
- Auditing is NOT security
- Compliance is NOT security
- The overwhelming majority of encryption is NOT security

- In all of the news reports about all of the break-ins and data thefts
- Have you ever heard or seen the following announced?

> Computers belonging to [name] were broken into, data on [###] billions of credit cards was stolen and it and the [company/organization] failed to pass compliance and security audits?

- You likely never will
- Victims of database breaches pass their audits ... proving audits and penetration tests are not relevant to securing data ... so what is?



Firewalls (1:4)

- Most organizations equate security with perimeter defense
- They have a firewall
- The following example is real and came from a customer security audit
- The firewall's configuration, discovered during the audit, allowed direct access from the internet to the database servers
- The organization's employees did not fully understand the implications of the rules they were writing

```
ICMP Allowed from outside to Business-Data Zone

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping match source-address any

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping match destination-address any

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping match application junos-ping

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping then permit

set security policies from-zone UNTRUST to-zone Business-Data policy BD-Ping then log session-close
```

Firewalls (2:4)

- The fact that a firewall has been purchased and configured should give you no sense of comfort
- Here is another firewall rule setting discovered during a security audit
- This example cancels the stateful feature of the firewall and make it just like a switch or router with security rules (ACLs)
- All traffic is allowed both from/to the outside interface with security level 0

```
dc-fwsm-app configurations

1094 access-list INBOUND-CAMPUS extended permit ip any any
3735 access-group INBOUND-CAMPUS in interface OUTSIDE
1096 access-list OUTBOUND-CAMPUS extended permit ip any any
3736 access-group OUTBOUND-CAMPUS out interface OUTSIDE

dc-fwsm-db configurations

access-list INBOUND-CAMPUS extended permit ip any any
access-group INBOUND-CAMPUS in interface OUTSIDE

access-list OUTBOUND-CAMPUS extended permit ip any any
access-group OUTBOUND-CAMPUS out interface OUTSIDE
```

The History of Perimeter Defense

- There is no wall that cannot be breached by a determined enemy
- The "impenetrable" Maginot Line was easily penetrated in WWI
- Firewalls are easily penetrated
- Identity Management is easily defeated ... I can defeat your LDAP system and so can you
- The only strategy that works is the one that has proven itself for thousands of years ... defense in depth

Breach exposes at least 58 million accounts, includes names, jobs, and more

With 2 months left, more than 2.2 billion records dumped so far in 2016.

DAN GOODIN - 10/12/2016, 2:29 PM

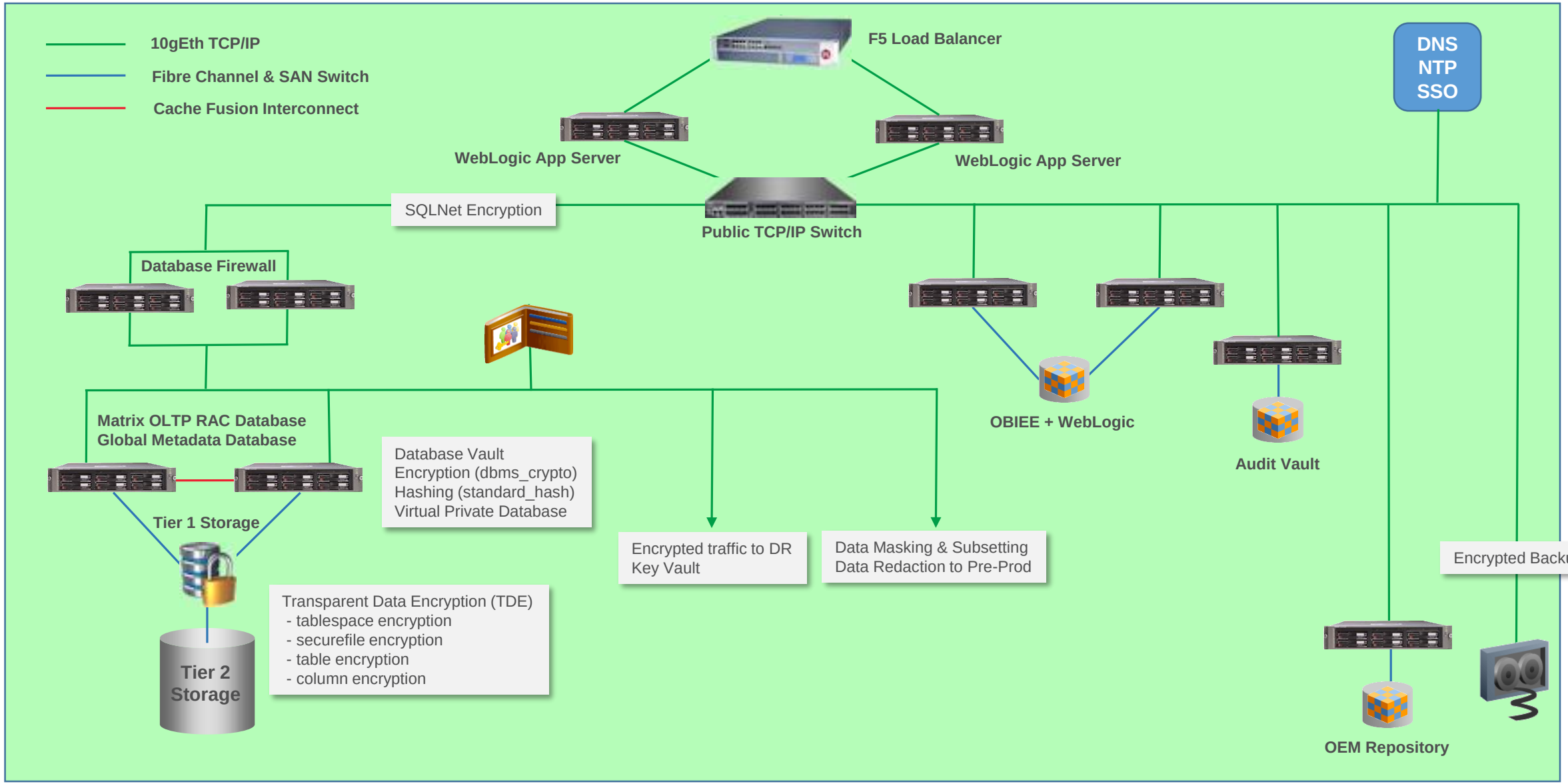
Firewalls (3:4)

- Every Oracle Database deployment requires multiple network connections

Name	Protocol	Utilization
Management	TCP/IP	System Admin connection to the server's light's-out management card
Public	TCP/IP	Access for applications, DBAs, exports, imports, backups: No keep-alive if RAC
SAN Storage	Fibre Channel	Server connection to a Storage Area Network (SAN)
NAS Storage	TCP/IP or IB	Connection to an NFS or DNFS mounted storage array
RAC Cache Fusion interconnect	UDP or IB	Jumbo Frames, no keep-alive, with custom configured read and write caching
Replication	TCP/IP	Data Guard and GoldenGate
Backup and Import/Export	TCP/IP	RMAN, DataPump, CommVault, Data Domain, ZFS, ZDLRA

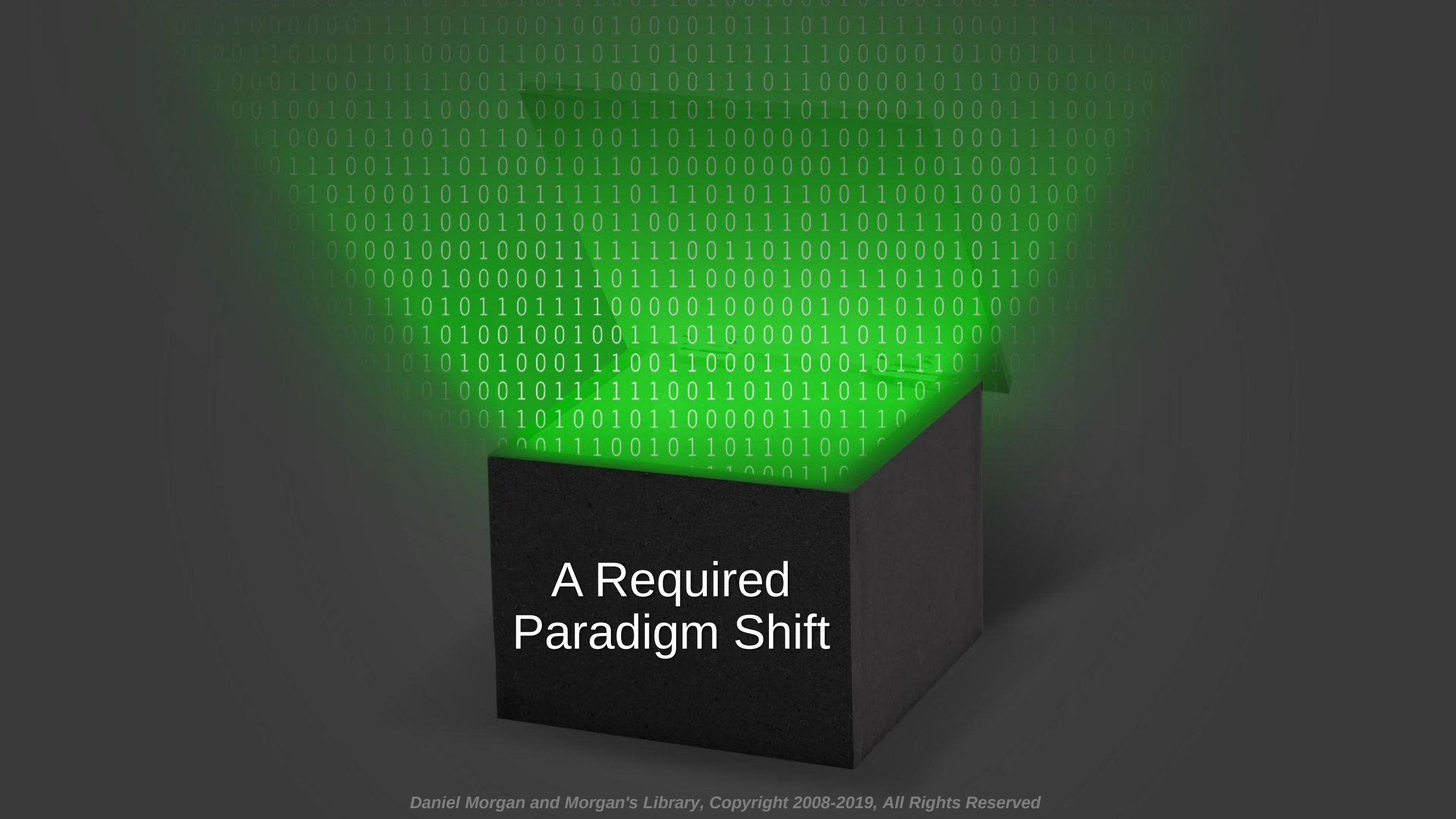
- Every one of these networks provides access to data
- No conversation on networking is complete without considering firewalls, DNS and NTP servers, load balancers, and a large variety of mobile and Internet of Things devices
- How many of the networks, above, go through the firewall?
- Probably only one of them ... the others probably shouldn't
- But each of them is an unmonitored vector for attack

Example of a Minimum Network Environment



Firewalls (4:4)

- Attempts are being made essentially 7 x 24 x 365 to attack your organization
- If you do not know this then you have insufficient monitoring and most likely many of the attempts have been successful
- A small division of one of America's largest retailers has not been able to identify a single 24 hour period in the last 5 years during which there was not at least one serious, professional, attempt to access their data



If Maxwell House Coffee is "good to the last drop"

- What's wrong with the last drop?
- Don't focus on what was said
- Focus on what should have been said but wasn't

Pay Attention To What Should Have Been Said ... But Wasn't

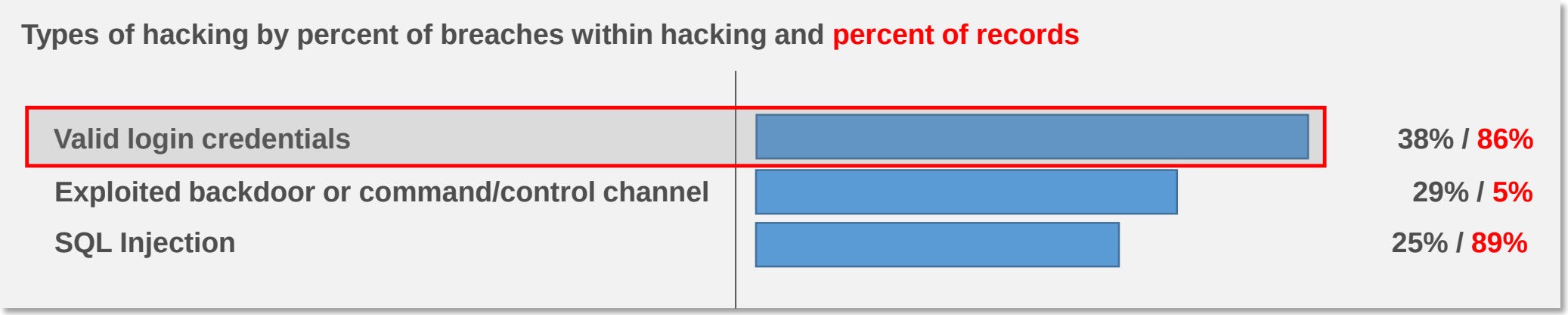
- Have you ever heard that an organizations that was the victim of a major breach failed an audit?

- Have you ever heard that any organization that was the target of a major breach configured all default security options correctly?

- Have you ever heard that any organization that was the target of a major breach applied all available and relevant security patches?

How Database Breaches Really Occur (1:2)

- 48% involve privilege misuse
- 40% result from hacking

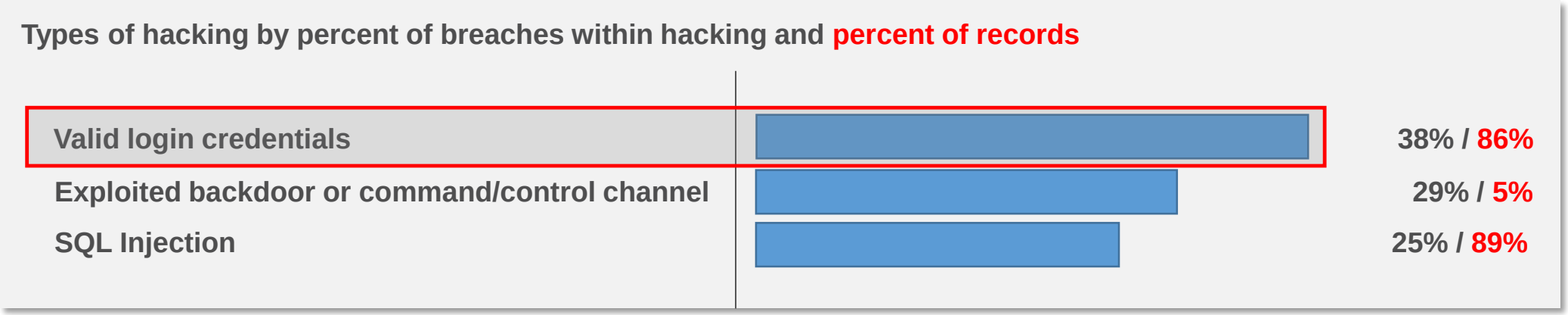


- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

Percentages do not add up to 100% because many breaches employed multiple tactics in parallel or were outliers

How Database Breaches Really Occur (2:2)

- 48% involve privilege misuse
- 40% result from hacking



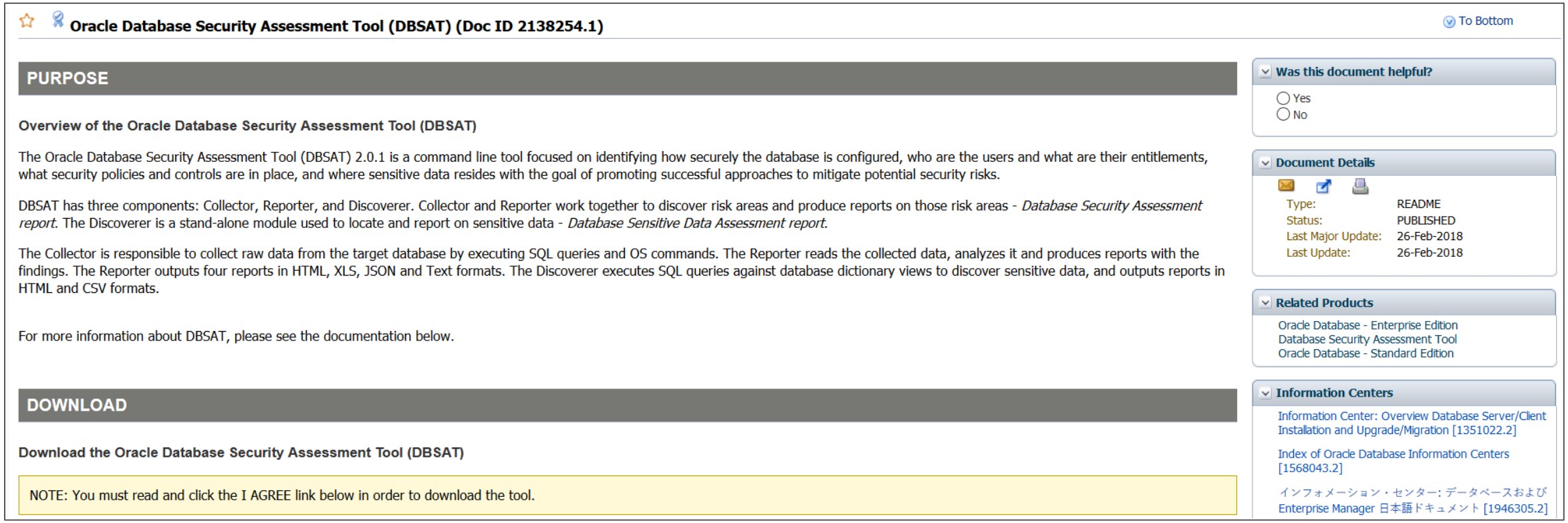
- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

How are you going to prevent access from someone that has a valid userid and password?

The correct answer is not MFA ... MFA can be defeated with a screw driver

We Are Often Misdirected By Our Suppliers and Vendors

- A great tool for selling Data Masking, Data Redaction, and Advanced Security Option
- Not so great at doing what its title says it does



Oracle Database Security Assessment Tool (DBSAT) (Doc ID 2138254.1)

To Bottom

PURPOSE

Overview of the Oracle Database Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool (DBSAT) 2.0.1 is a command line tool focused on identifying how securely the database is configured, who are the users and what are their entitlements, what security policies and controls are in place, and where sensitive data resides with the goal of promoting successful approaches to mitigate potential security risks.

DBSAT has three components: Collector, Reporter, and Discoverer. Collector and Reporter work together to discover risk areas and produce reports on those risk areas - *Database Security Assessment report*. The Discoverer is a stand-alone module used to locate and report on sensitive data - *Database Sensitive Data Assessment report*.

The Collector is responsible to collect raw data from the target database by executing SQL queries and OS commands. The Reporter reads the collected data, analyzes it and produces reports with the findings. The Reporter outputs four reports in HTML, XLS, JSON and Text formats. The Discoverer executes SQL queries against database dictionary views to discover sensitive data, and outputs reports in HTML and CSV formats.

For more information about DBSAT, please see the documentation below.

DOWNLOAD

Download the Oracle Database Security Assessment Tool (DBSAT)

NOTE: You must read and click the I AGREE link below in order to download the tool.

Was this document helpful?

Yes
No

Document Details

Type:	README
Status:	PUBLISHED
Last Major Update:	26-Feb-2018
Last Update:	26-Feb-2018

Related Products

Oracle Database - Enterprise Edition
Database Security Assessment Tool
Oracle Database - Standard Edition

Information Centers

Information Center: Overview Database Server/Client Installation and Upgrade/Migration [1351022.2]

Index of Oracle Database Information Centers [1568043.2]

インフォメーション・センター: データベースおよび Enterprise Manager 日本語ドキュメント [1946305.2]

First Paradigm Shift

- To be successful you must accept that ...

Break-ins will occur.

Those who fail to study history are doomed to repeat it.

Second Paradigm Shift

- To be successful you must accept that ...

```
Your job is to increase the difficulty for those breaking in.
```

If your management doesn't grasp this reality then it is your responsibility to explain it to them.

Securing existing databases is more important than deploying more insecure databases.

Third Paradigm Shift

- To be successful you must accept that ...

The database must be configured to limit the damage.

On Installation
- Disable the DEFAULT profile
- Revoke almost all privileges granted to PUBLIC
- Enable all of the database's default security capabilities

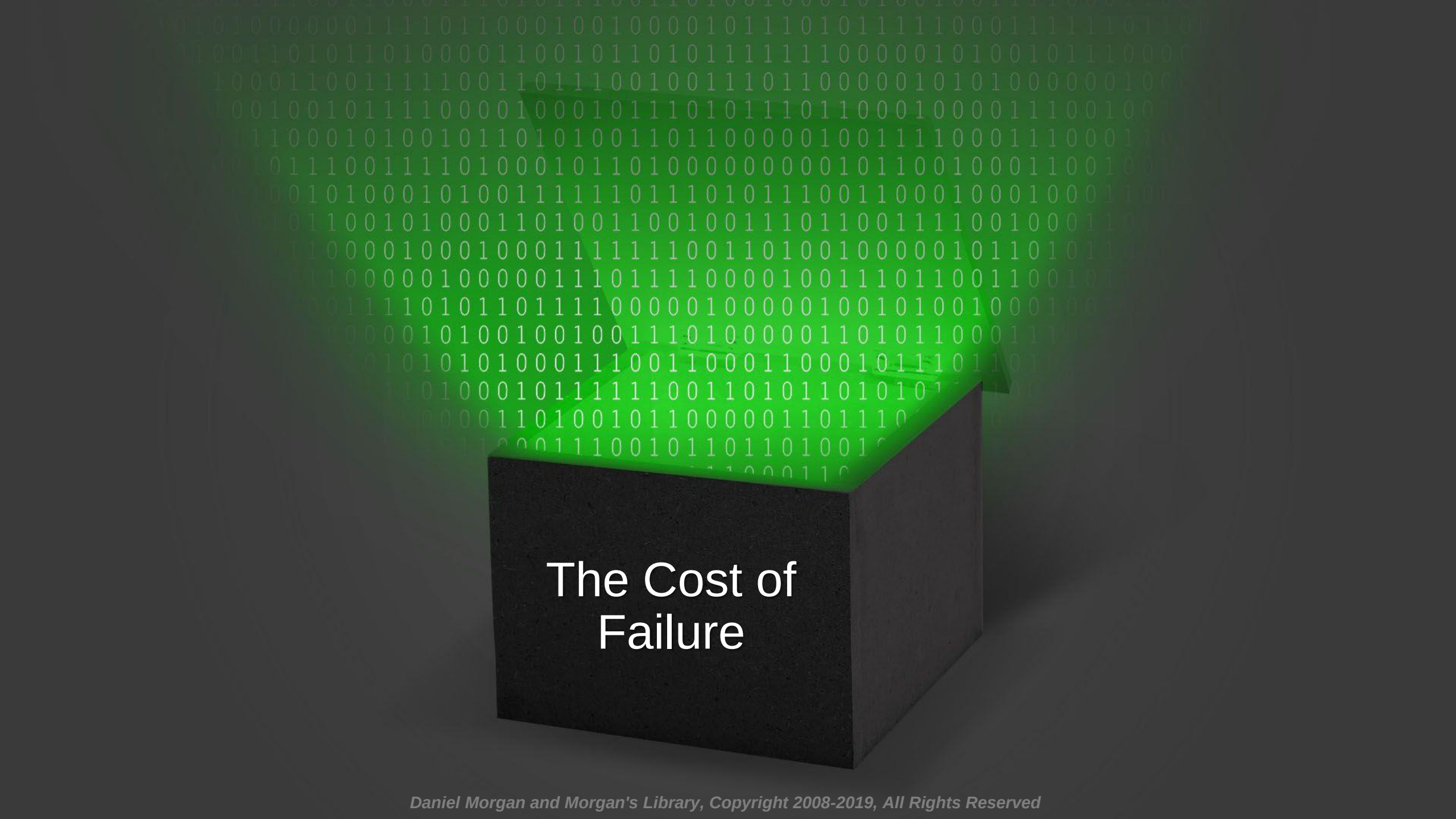
After Installation
- Apply security patches immediately
- Stop using cron - use DBMS_SCHEDULER
- Change passwords regularly - automate the process
- Do not grant the CONNECT, RESOURCE, or DBA roles ever
- Use Proxy Users for every connecting user you create
- Implement Database Vault
- Implement Row Level Security

- There is always someone inside the firewall
- There is always someone with access
- There is a big difference between accessing one record ... and accessing everything
- Most databases in the are configured so that once someone breaks in they get everything
- Make it impossible to SELECT all rows

What You Are Going To Learn Today

Go To Labs

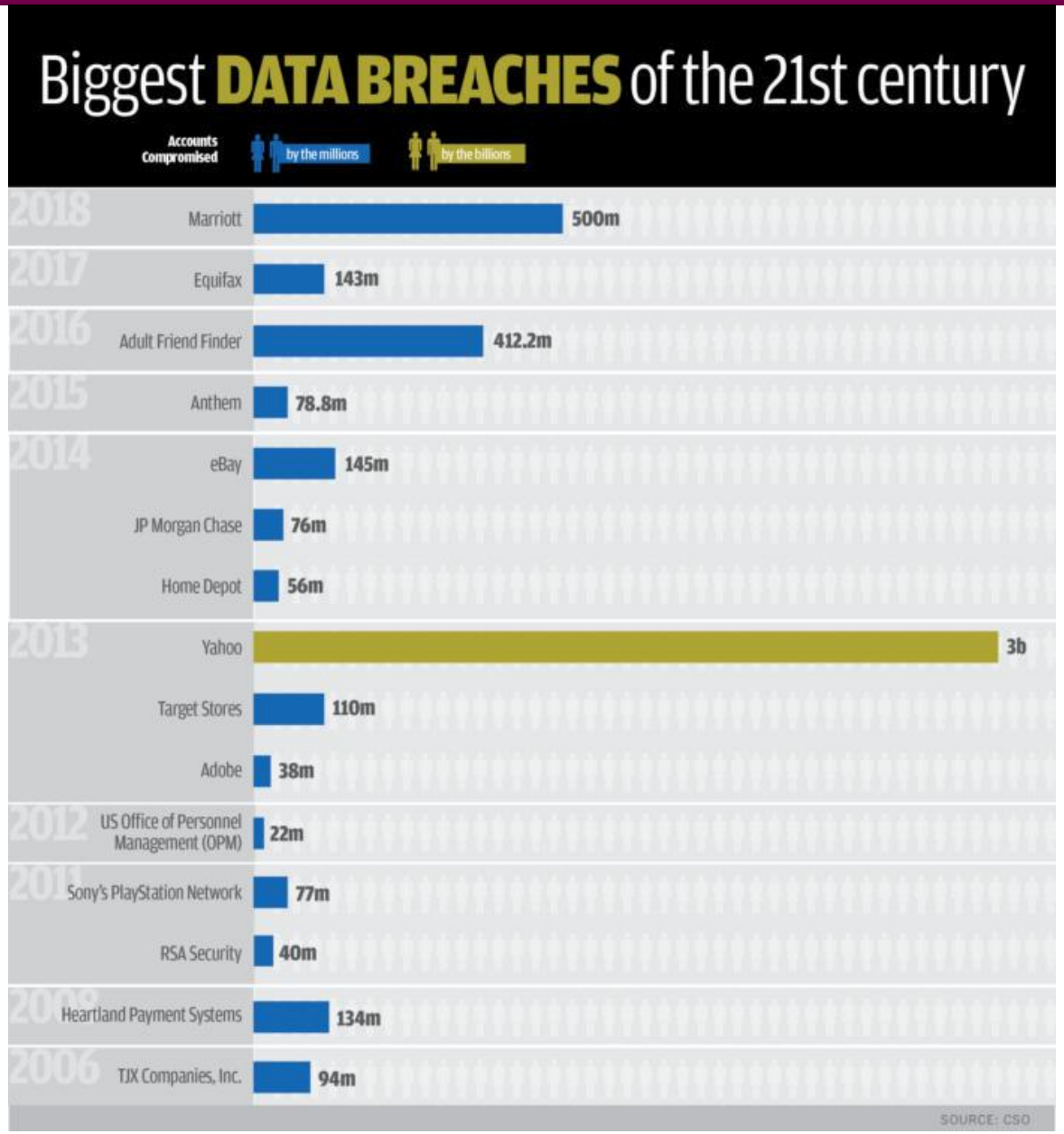
- To protect data you must secure databases
- Perimeter defense, alone, is of little value
- Data security, for some products, means protecting database access
- Security with other database products is more difficult to achieve
- Today we will use an Oracle Database
  - On a laptop
  - Not connected to an organization's network
  - Without a valid userid and password
  - To attack the an organization
- All commercial and open source databases are, by default, insecure
  - The same basic skill set than can compromise Oracle will compromise SQL Server, MongoDB, Cassandra, PostgreSQL, MySQL, all of them
  - The specific vulnerabilities may be different
  - The specific exploit and syntax may be different
  - **It is the thought process and the concepts** that create a successful attack



Getting It Wrong

- One reason we do not have good security is the perception by management that it is expensive ... they could not be more wrong
- The cost of properly implementing good security should be close to neutral
- I am not in sales
- I do not sell a single hardware or software product related to anything we will be discussing today
- The reason security appears to be expensive is that most people ask account executives, people that sell products, what to do
- And, by an amazing coincidence, their answer always corresponds to the fact that the more you buy of what they just happen to be selling the more secure you will be
- This is not to say buying some of these products isn't important ... it is
- Pass audits is important and measurable ... but it does not secure data
- The overwhelming majority of organizations that take locking down their data and databases seriously ... save money

Which Is Why We Have Charts Like This



Some Background

Background

Hackers and criminal insiders cause the most data breaches. Forty-seven percent of all breaches in this year's study were caused by malicious or criminal attacks. The average cost per record to resolve such an attack was $156. In contrast, system glitches cost $128 per record and human error or negligence is $126 per record. Companies in the United States and Canada spent the most to resolve a malicious or criminal attack ($244 and $201 per record, respectively). India spent far less ($78 per record).

Did you catch ... "per capita"?

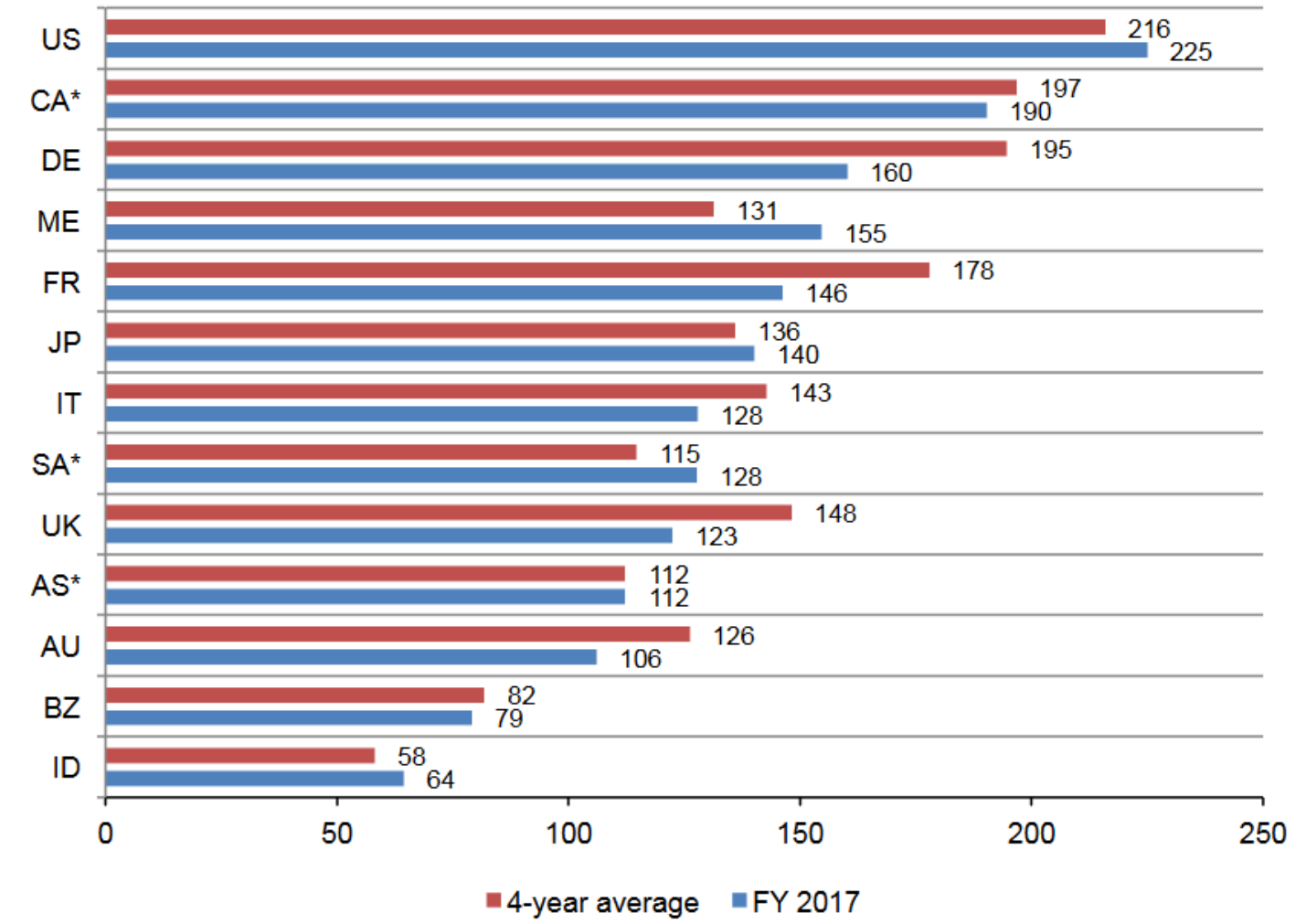
Data breaches are most expensive in the United States and Canada and least expensive in Brazil and India. The average per capita cost of data breach was $225 in the United States and $190 in Canada. The lowest cost was Brazil ($79) and India ($64). The average total organizational cost in the United States was $7.35 million and $4.94 million in the Middle East. The lowest average total organizational cost was in Brazil ($1.52 million) and India ($1.68 million).

The faster the data breach can be identified and contained, the lower the costs. For the third year, our study reports the relationship between how quickly an organization can identify and contain data breach incidents and the financial consequences. For our consolidated sample of 419 companies, the mean time to identify (MTTI) was 191 days with a range of 24 to 546 days. The mean time to contain (MTTC) was 66 days with a range of 10 to 164 days. Both the time to identify and the time to contain were highest for malicious and criminal attacks (214 and 77 days, respectively) and much lower for data breaches caused by human error (168 and 54 days, respectively).

The more records lost, the higher the cost of the data breach. Cost analysis reveals a relationship between the average total cost of data breach and the size of the incident. In this year's study, the average total cost ranged from $1.9 million for incidents with less than 10,000 compromised records to $6.3 million for incidents with more than 50,000 compromised records. Last year the cost ranged from $2.1 million for a loss of less than 10,000 records to $6.7 million for more than 50,000 records.

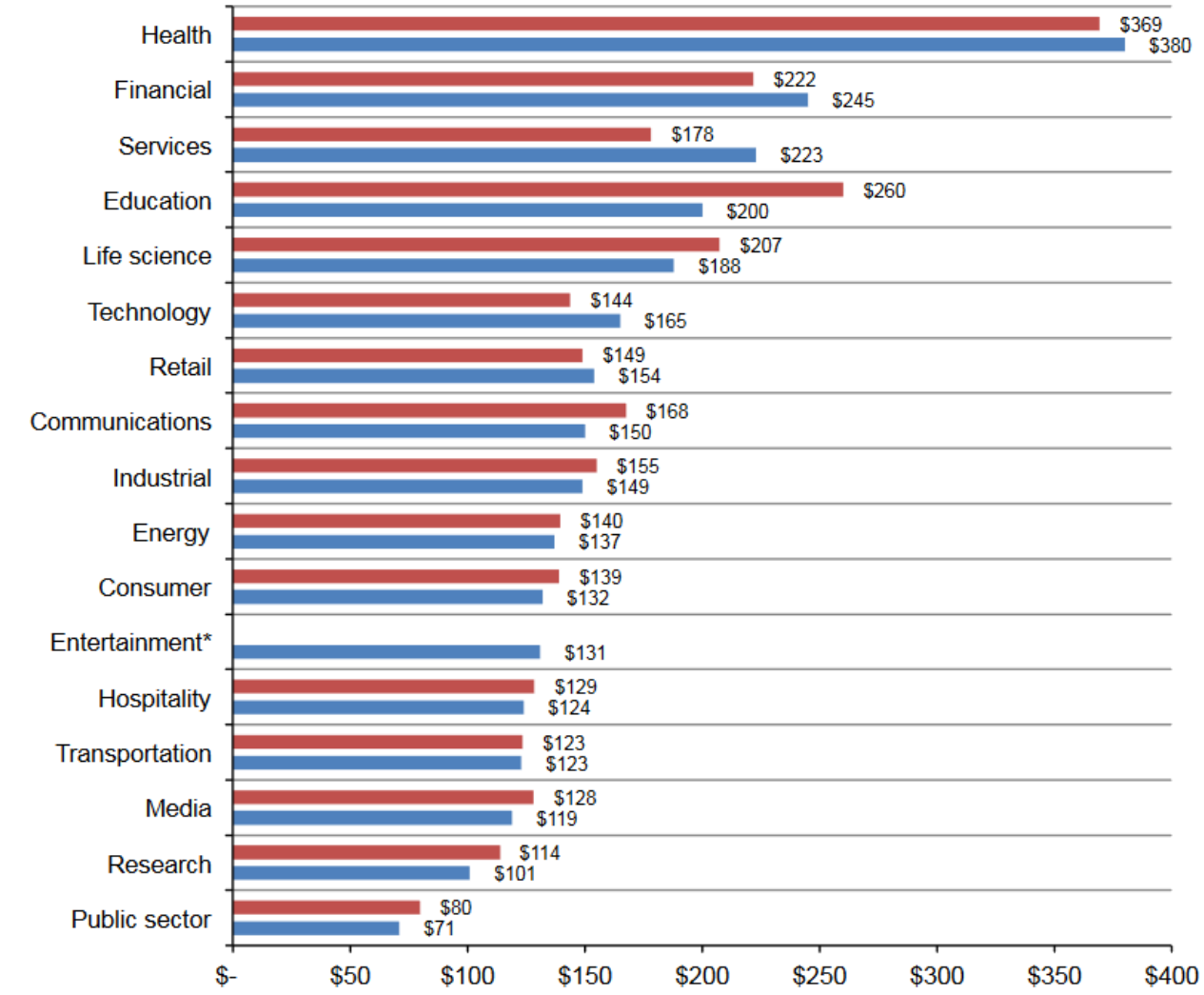
Background

Figure 1. The 2017 per capita cost of data breach compared to the four-year average
Grand averages for FY2017=$141, FY2016=$158, FY2015=$154, FY2014=$145
*Historical data are not available for all years
Measured in US$



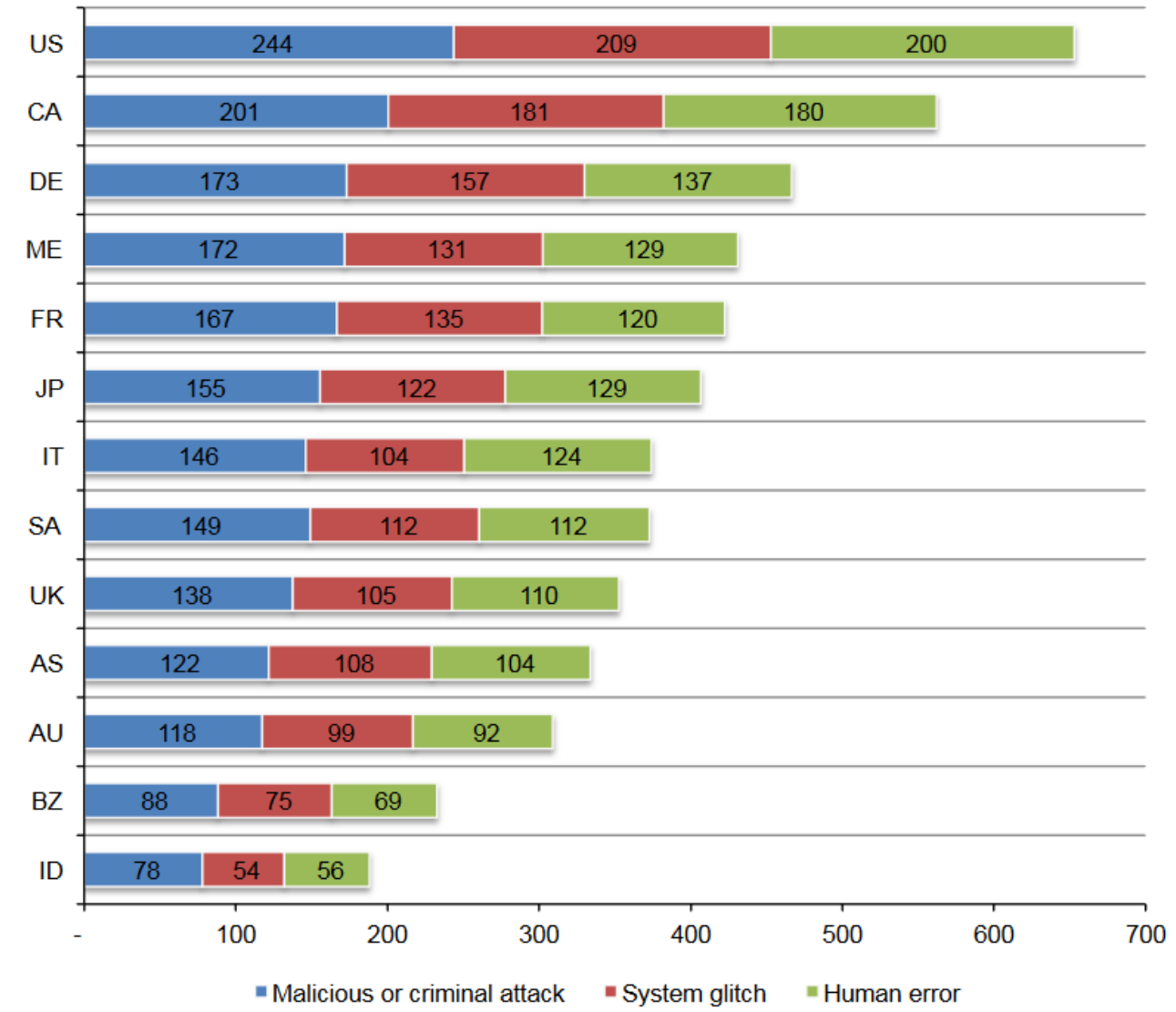
Background

Figure 5. Per capita cost by industry classification
*Historical data are not available for all years
Measured in US$

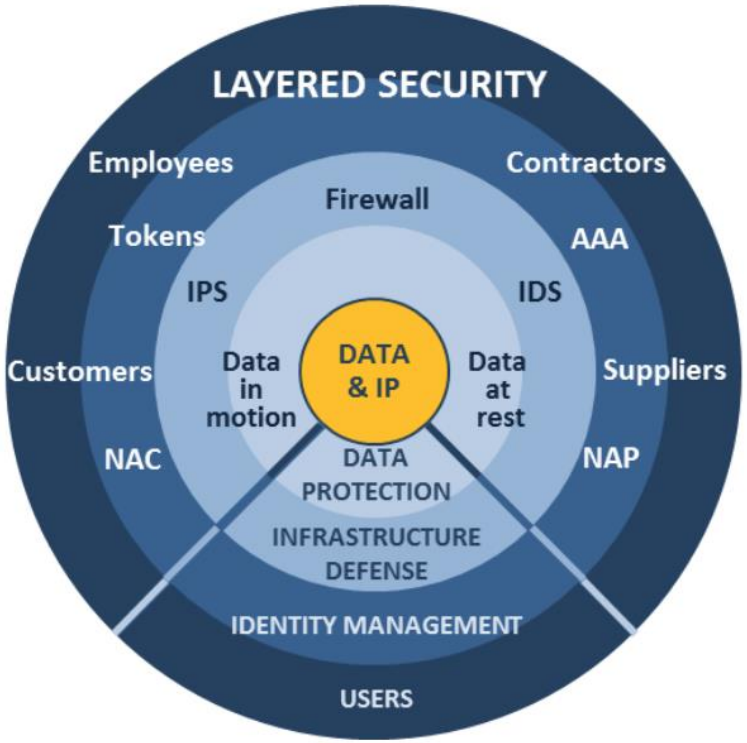


Background

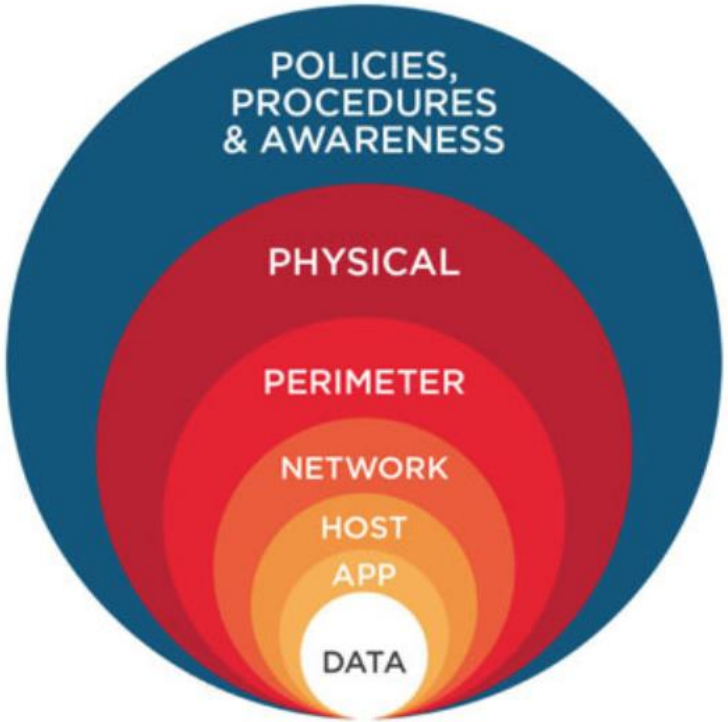
Figure 8. Per capita cost for three root causes of data breach by country and region
Measured in US$

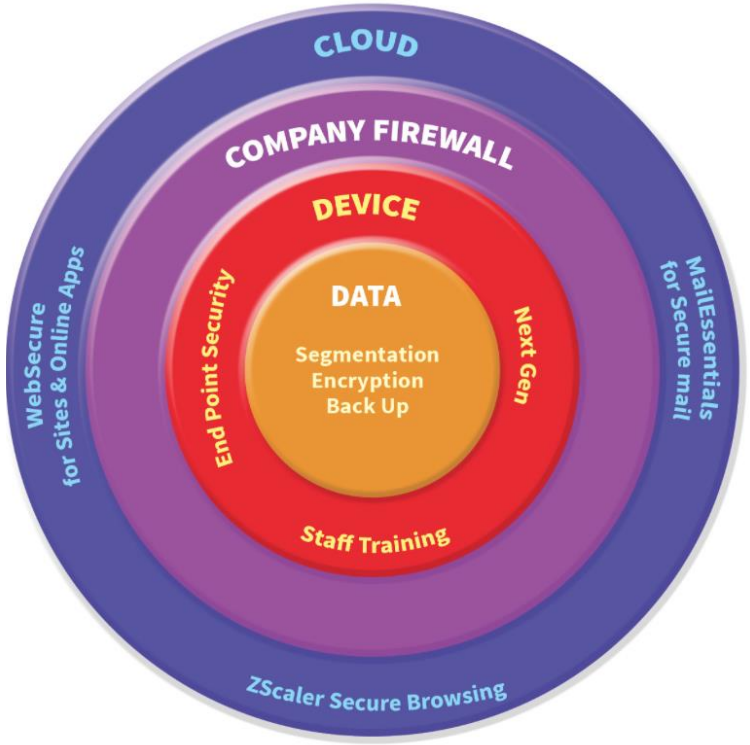


Defense in Depth

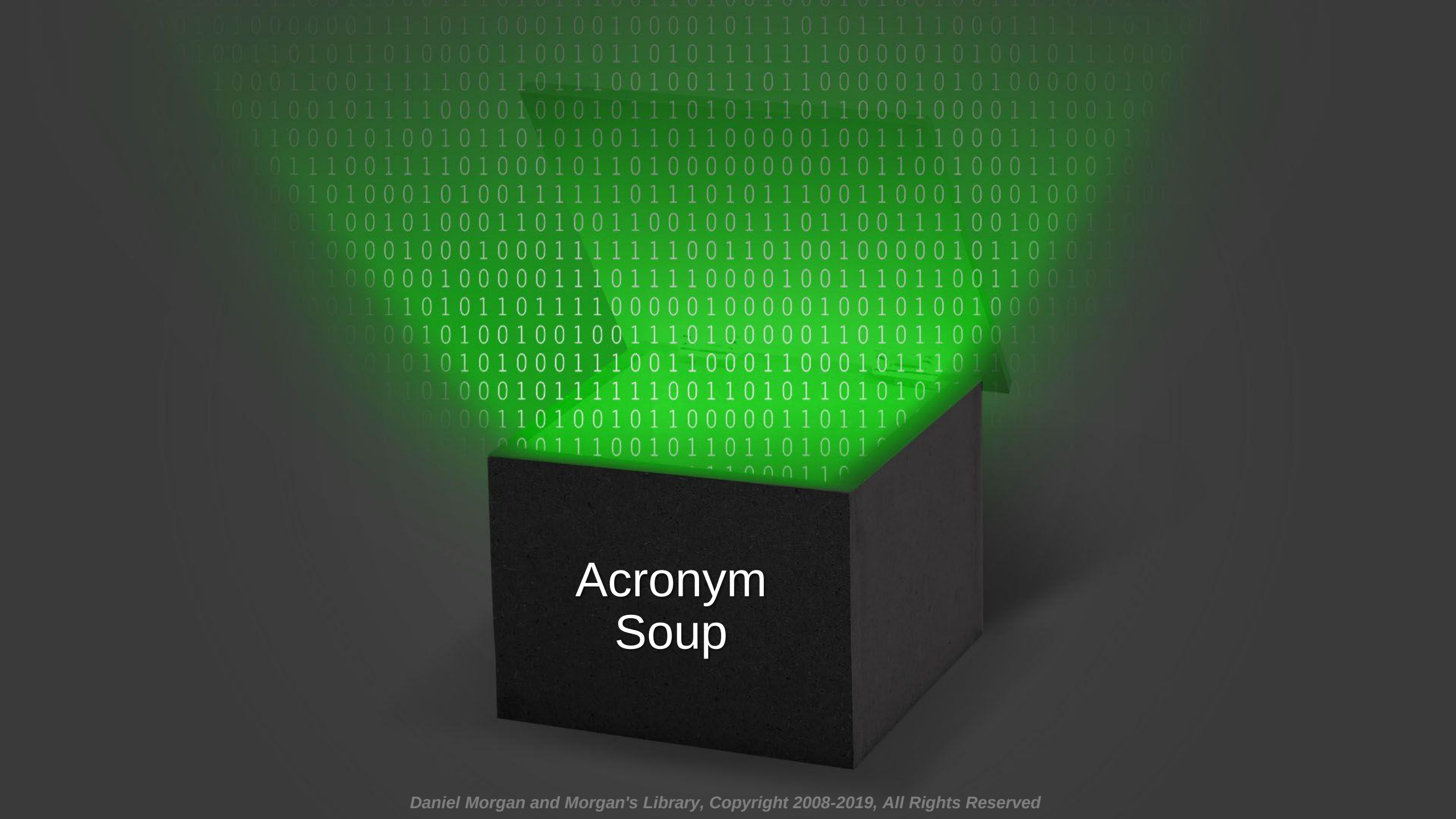


What each of these drawings, from different sources, has in common is that the data is that which must be protected

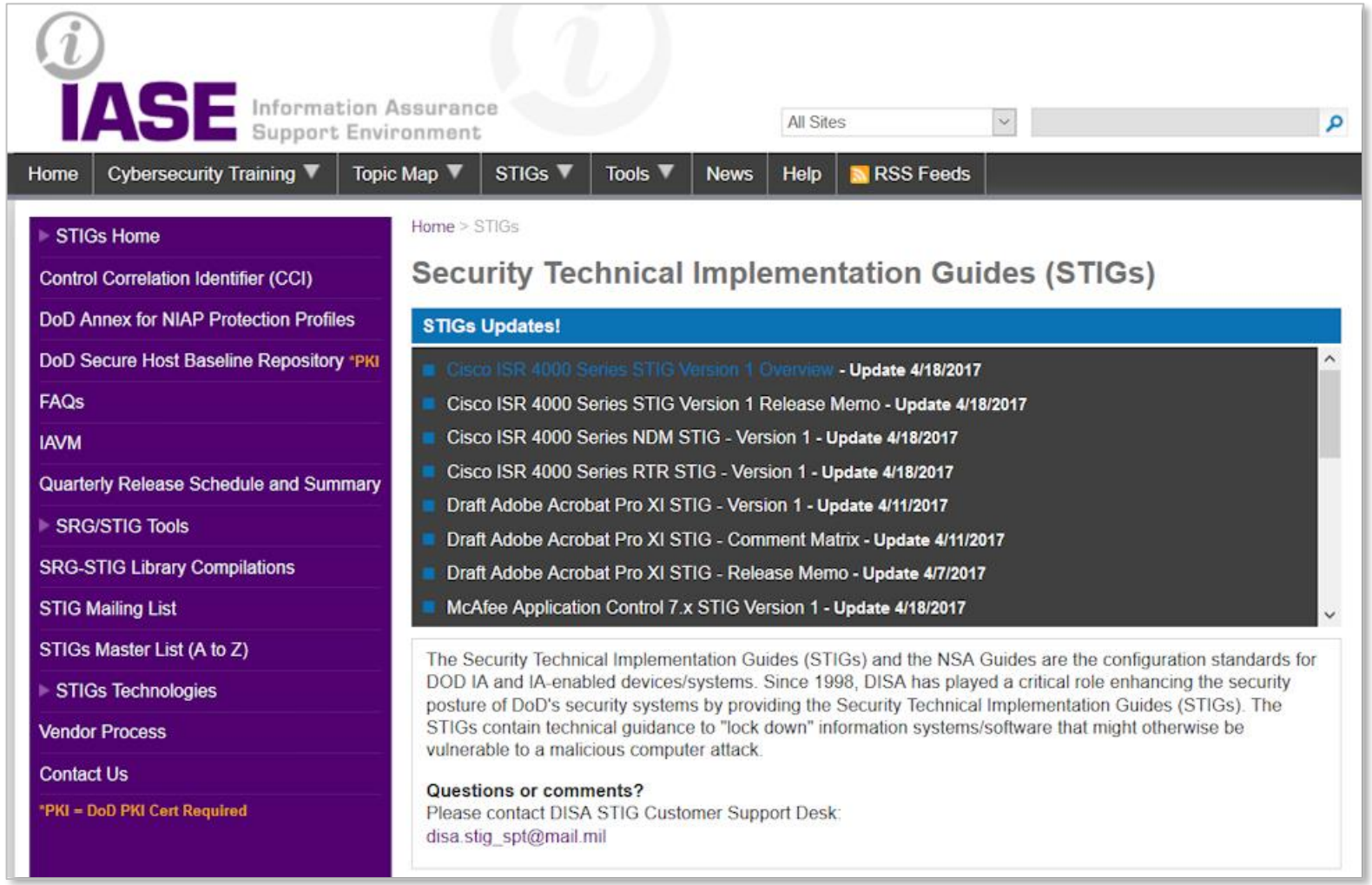




If no one can get into your network, but they can still get to your data, you lose the game ... and there are no replays

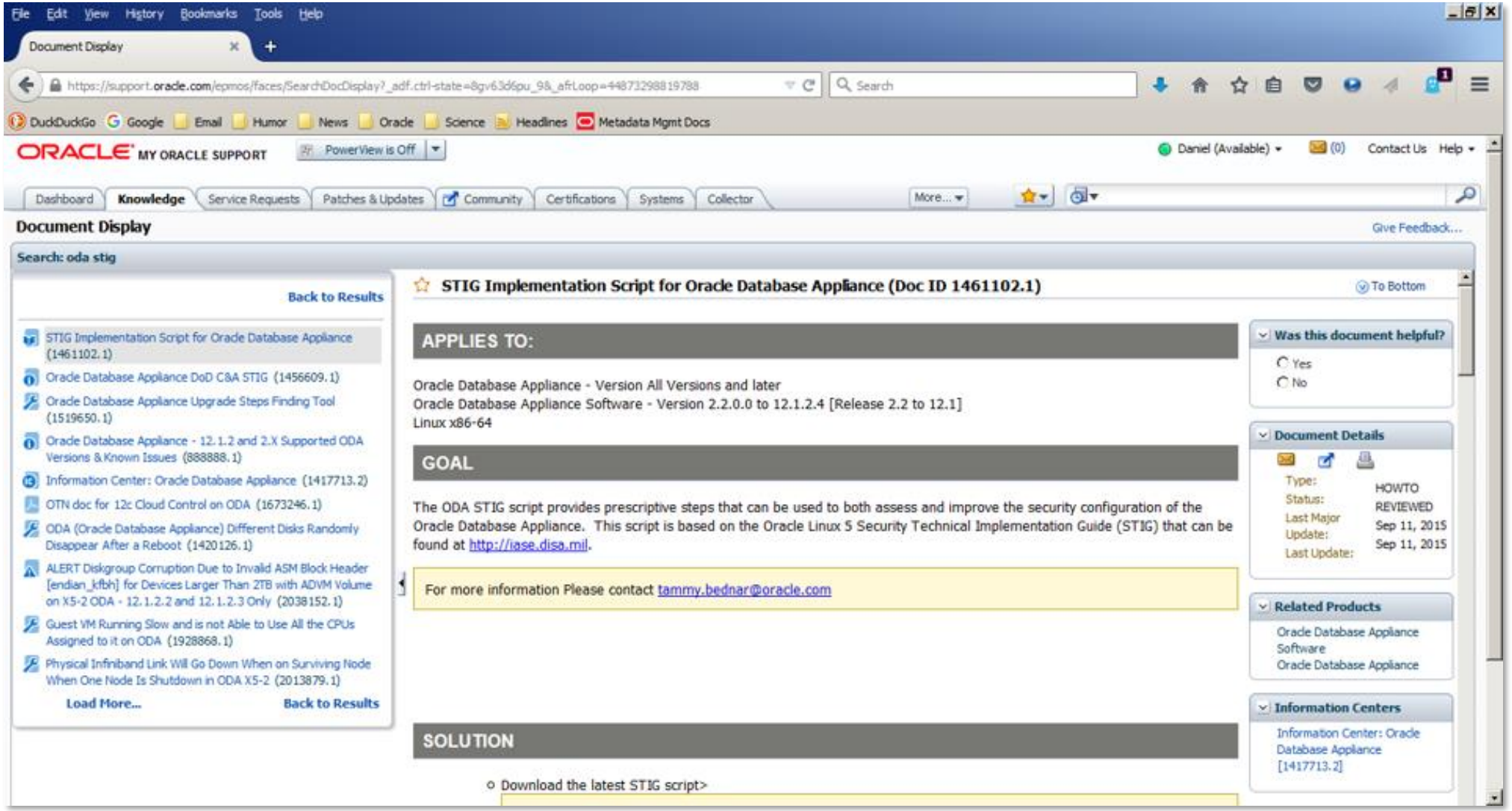


STIG (1:3)



`http://iase.disa.mil/stigs/Pages/index.aspx`

STIG (2:3)



STIG (3:3)

- A STIG is a Security Technical Implementation Guide produced or approved by the US Department of Defense
- Oracle has published STIGs at My Oracle Support for Exadata and ODA
  - But the "CHECK" option can be run on any Linux server
- Oracle Support provides a downloadable script that can be used to check an ODA against STIG requirements and identify three levels of violations
- We strongly recommend running the script with the **`-check`** option but recommend having your Linux System Admin correct those issues you wish to correct manually

Warning: Never run the STIG script with the -fix option

- Ctrl-Alt-Del combination to shutdown system is enabled
- Password for grub not enabled
- Privilege account 'halt' is present
- Privilege account 'shutdown' is present
- RealVNC rpm is installed on system
- sendmail decode command is not commented in /etc/aliases
- Support for USB device found in kernel

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT

DFARS (2:2)

- This is NOT a security document

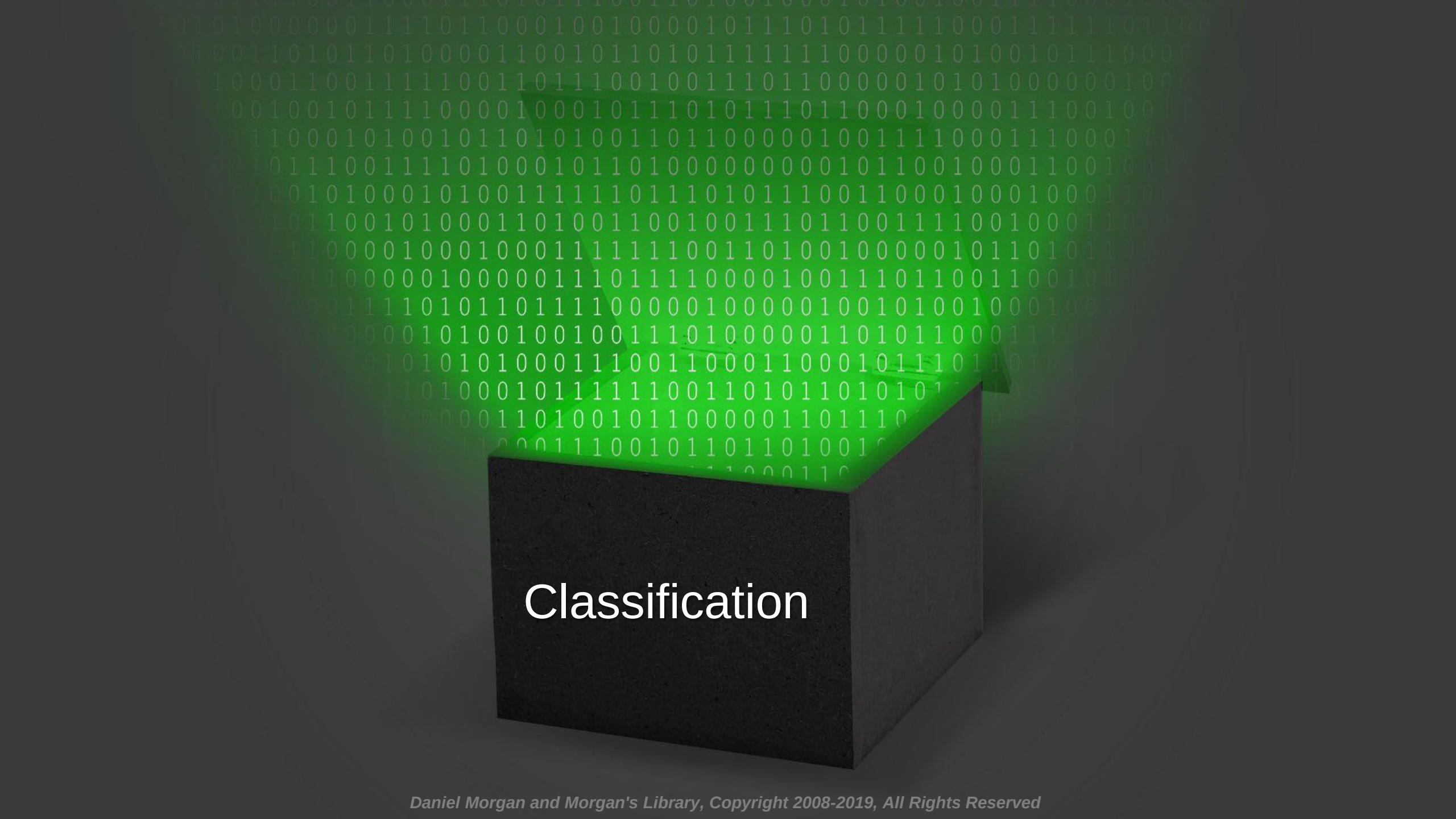
Defense Federal Acquisition Regulation Supplement

Table of Contents

Center for Internet Security (CIS)

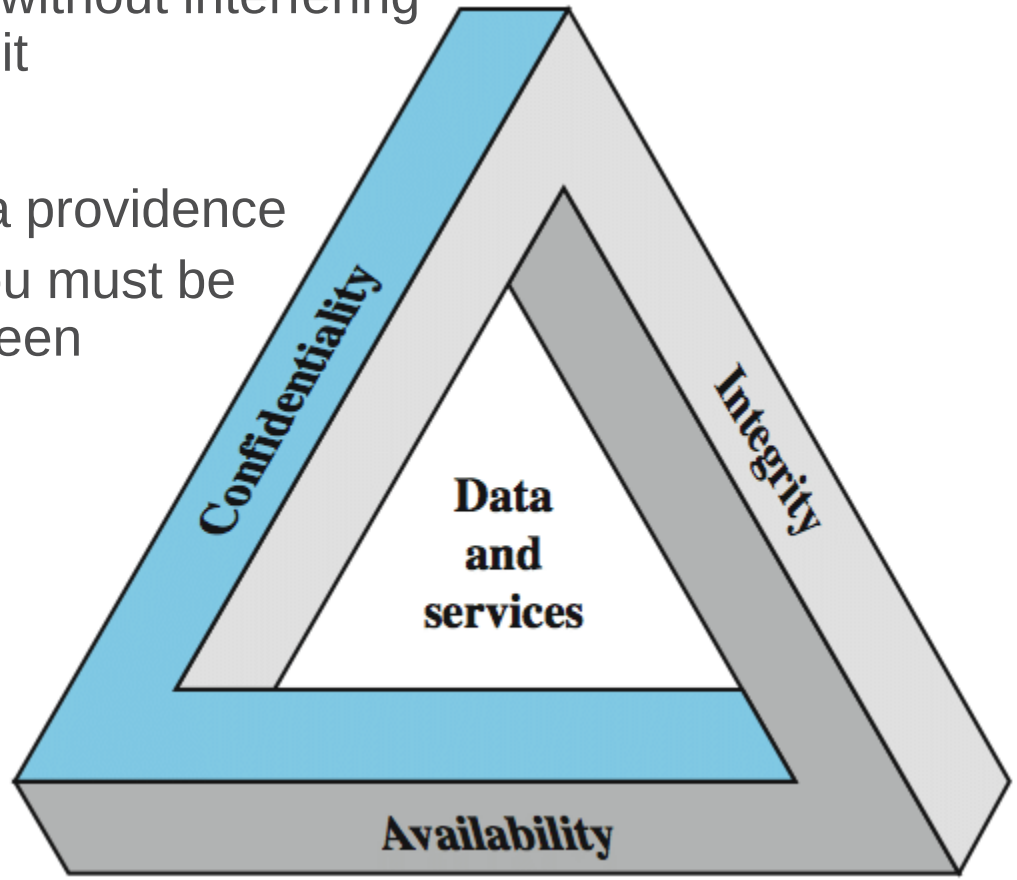
- CIS is the source of audit guidelines and auditors for many e-commerce websites

`https://www.cisecurity.org`



CIA Triangle

- Confidentiality
  - Disclosure/Privacy
  - Actions taken to ensure confidentiality are those designed to prevent **sensitive information** from reaching the wrong people without interfering with the ability of the correct people to access it
- Integrity
  - Actions taken to ensure data integrity and data providence
  - Like the chain-of-custody in a criminal case you must be able to establish its origin and that it has not been altered or specifically when, where, and how it was altered
- Availability
  - For data to be available you must have a high availability stable environment with infrastructure and data redundancy, usable backups, DDOS protection, and adequate bandwidth



Classification

- The critical phrase under "Confidentiality" in the CIA triangle is "sensitive information"
- It implies that you know what is sensitive
- The overwhelming majority of organizations have never taken even the first step required to identify what information is sensitive
- Classification is the process by which we identify what is sensitive
- No one has infinite resources so no one can fully protect every thing we must start our effort by defining the following
  - What are we trying to protect?
  - What are we going to protect it from?
  - How much risk are we willing to accept?
  - How will be quantify our objective
  - How will we mitigate the risk?
- **Is a comments field sensitive?**

Overview of Classification Objectives

- We want to assign each application an appropriate classification
- We need to apply our knowledge of the business to the classification, as well sa our IT stewardship
  - This is an initial classification, and will need to eventually be reviewed with the business
- Classifications are baesd on what we think they should be, not what the current infrastructure supports
  - Need to document what challenges might exist in implementing the appropriate classification
- The classification guidelines are intended to define both HA and DR requirements
  - There will be some exceptions to this linkage

Classification: What Are We Trying To Protect?

- <Let's fill this out>

Classification: What Are We Going To Protect It From?

- <Let's fill this out>

Classification: How Much Risk Are We Willing To Accept?

- <Let's fill this out>

Classification: How Will We Quantify Our Objective?

- <Let's fill this out>

Classification: How Will We Mitigate The Risks?

- <Let's fill this out>

Typical Application Breakdown

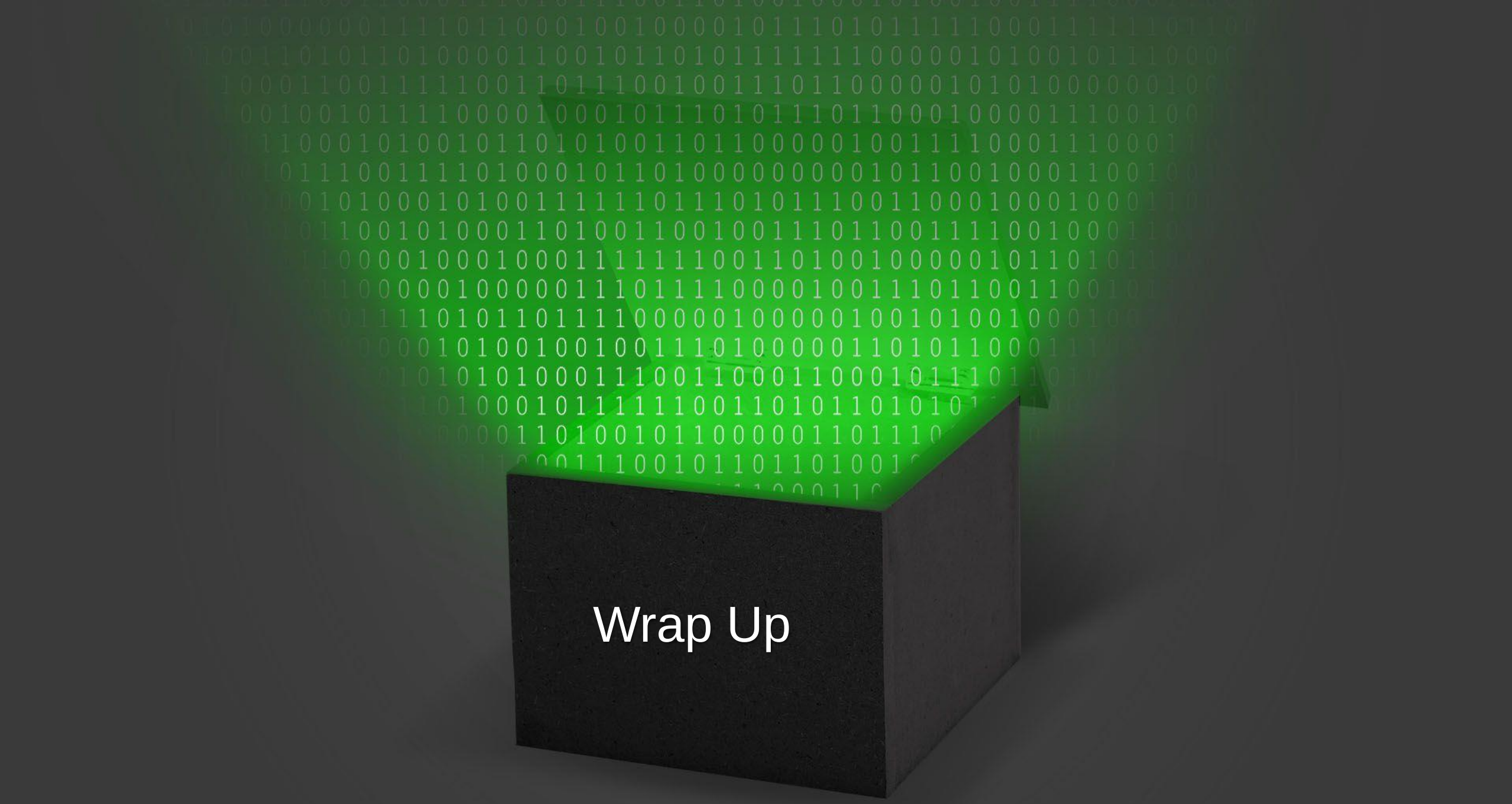
Risk Type	Risk Source	Identification	Location	Mitigation Type	Risk Score
Theft	Internal	TABLE_NAME	File System Name	Identity Management	A
Insertion	External	COLUMN_NAME	Database Name	Encryption	B
Modification	Employee	FILE NAME	Data Center	Multi-Factor Authentication	C
Deletion	Vendor	Preproduction DB	Colo	Firewall	D
Attack Vector	Contractor	Backup Tape	Vault	No Authentication Schema	Z

Factors to Consider

- The following items are characteristics of an application that need to be considered when determining the appropriate Application Classification
  - Financial Loss
    - Potential loss or harm to monetary expenditures and receipts
    - Includes profit loss, interest loss, fees, fines, penalties, portfolio management, fee income, financial liabilities, etc.
  - Regulator/Legal
    - Loss due to non-compliance or adherence to laws, ordinances, statutes, SLA's, and/or contracts
  - Customer Service
    - Activities designed to support customer needs before, during and after a customer purchase or provided service
    - Can include external and internal customers and employees
  - Reputation
    - How <organization_name> is perceived by customers, media, outside organizations, and employees
    - Can be associated with the company's achievements, attainments, integrity, trustworthiness, reliability, customer focus, etc.

Definitions: RTO / RPO

- RTO - A Recovery Time Objective is the amount of time that an application, system or piece of infrastructure is expected (or allowed) to be unavailable once a disaster has been declared
- RPO - A Recovery Point Objective is the acceptable amount of data loss that occurs during a disaster event - more specifically, the time between the last backed up data and the time of the disaster
  - May also include logs and files that may be applied subsequent to the last backup



Both of These Train Wrecks Were Avoidable

```
DIR=/opt/oracle/scripts
. /home/oracle/.profile_db

DB_NAME=hrrpt
ORACLE_SID=$DB_NAME"1"
export ORACLE_SID

SPFILE=`more $ORACLE_HOME/dbs/init$ORACLE_SID.ora | grep -i spfile`
PFILE=$ORACLE_BASE/admin/$DB_NAME/pfile/init$ORACLE_SID.ora
LOG=$DIR/refresh_$DB_NAME.log
RMAN_LOG=$DIR/refresh_$DB_NAME"_rman".log

PRD_PWD=sys_pspr0d
PRD_SID=hrprd1
PRD_R_UNAME=rman_pshrprd
PRD_R_PWD=pspr0d11
PRD_BK=/backup/hrprd/rman_bk
SEQUENCE=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $5 }'`
THREAD=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $4 }'`

BK_DIR=/backup/$DB_NAME/rman_bk
EXPDIR=/backup/$DB_NAME/exp
DMPFILE=$EXPDIR/exp_sec.dmp
IMPLOG=$EXPDIR/imp_sec.log
EXPLOG=$EXPDIR/exp_sec.log
EXP_PARFILE=$DIR/exp_rpt.par
IMP_PARFILE=$DIR/imp_rpt.par

uname=rman_pshrprd
pwd=pspr0d11

rman target sys/$PRD_PWD@$PRD_SID catalog $PRD_R_UNAME/$PRD_R_PWD@catdb auxiliary / << EOF > $RMAN_LOG
  run{
     set until $SEQUENCE $THREAD;
     ALLOCATE AUXILIARY CHANNEL aux2 DEVICE TYPE DISK;
     duplicate target database to $DB_NAME;
  }
EOF
```

```
$ find "pwd" *
$ grep -ril "pwd" /app/oracle/*
$ ack pwd
```

Conclusions (2:3)

- It is difficult to dig yourself out of a hole after the sides have fallen in
- Very few organizations have employees with the skill set required to secure their databases and operational environments: Less than 1% of DBA "training" involves security
- If you don't have the internal skills to know what to protect and how to protect it you need to go outside your organization and ask for help

Our New Reality

- There isn't a lot of room in IT for Conscientious Objectors

Minimum Secure Environment (1:4)

- All non-essential schemas dropped
- All Oracle provided schemas have non-default passwords and are locked
- All administrative users log in with proxy accounts that are personally identifiable and audited and have their privileges granted with a role that provides only the system and object privileges they require to do their job
- The Default profile is modified so that it has insufficient resources to do anything
- Every connection created is a proxy user including DBAs
- Every profile is a customized profile that limits logins, forces password complexity, performs automatic logoffs for inactive time and excess connection time
- Only necessary privileges are granted
- All privileges of DBA_ objects to PUBLIC are dropped by default
- All privileges of ALL_SOURCE and USER_SOURCE views to PUBLIC are dropped by default

Minimum Secure Environment (2:4)

- All databases 12c and above are created by installation and not by upgrade
- No system privilege that contains the word ANY is granted to anyone without a written justification
- No one gets execute privilege on DBMS_SYS_SQL
- A Network Access Control list is configured inside every database
- A daily report is produced and reviewed of users with default passwords
- All internal applications that contain calls to DBMS_SQL or EXECUTE IMMEDIATE must contain calls to DBMS_ASSERT to force enquoting
- All objects in $ORACLE_HOME/rdbms/admin are read only
- A job run by a shell script owned by root checks the entire file system once each day for any file that contains passwords
- All jobs that connect to a database run by shell scripts are converted to be run by DBMS_SCHEDULER
- Drop all unnecessary DIRECTORY objects

Minimum Secure Environment (3:4)

- Use DBMS_DISTRIBUTED_TRUST_ADMIN to disable all database links unless the connection is explicitly authorized
- Wrap Up
  - Governance, Compliance, Auditing, passing Audits is an essential part of your job responsibility
  - But it does not make data or databases more secure
  - To secure databases criteria must be current ... updated no less frequently than every 90 days
  - To secure databases you must hire experts that know how to attack them
  - To secure databases you must deploy them in a secure configuration and monitor for changes
  - To secure databases you must change how you do things
  - And if you do them correctly you should save a substantial amount of money

Minimum Secure Environment (4:4)

- Homework
  1. Of the resources you manage, whatever they may be, list the top 3 unaddressed vulnerabilities that would allow someone to compromise high priority data
  2. Write down the top 3 roadblocks standing in your way of fixing these vulnerabilities in the next 24 hours

  You will be the only person looking at these lists tomorrow morning ... you will not be asked to share them with anyone.

Conclusions

- Success requires that we develop a new approach to our jobs
- That we reprioritize securing existing systems over creating additional insecure systems
- We must lead our employers to an understanding that passing audits is not sufficient
- And that we implement no new feature before we understand the potential risks

```
SELECT more_information
FROM experience
WHERE tool = 'Oracle Database'
AND topic = 'Security';
```

email: damorgan@dbsecwork.com
web: www.dbsecworx.com
www.morganslibrary.org

Thank you