



Oracle Security for DBAs and Developers

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



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?

KrebsOnSecurity

In-depth security news and investigation



[ADVERTISING/SPEAKING](#) [ABOUT THE AUTHOR](#)

[A Little Sunshine / Data Breaches](#) — 7 comments

31 NY Investigates Exposure of 885 Million Mortgage Documents

MAY 19

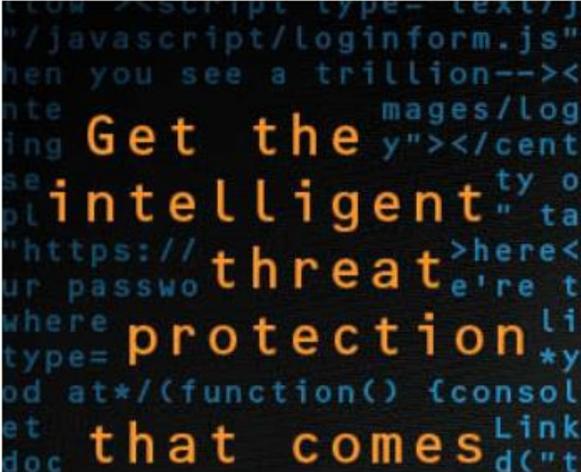
New York regulators are investigating a weakness that exposed 885 million mortgage records at **First American Financial Corp.** [NYSE:FAF] as the first test of the state's strict new cybersecurity regulation. That measure, which went into effect in March 2019 and is considered among the toughest in the nation, requires financial companies to regularly audit and report on how they protect sensitive data, and provides for fines in cases where violations were reckless or willful.

On May 24, KrebsOnSecurity **broke the news** that First American had just fixed a weakness in its Web site that exposed approximately 885 million documents — many of them with Social Security and bank account numbers — going back at least 16 years. No authentication was needed to access the digitized records.



Mailing List

[Subscribe here](#)



How Well Do You Know Oracle?

```
SELECT (columns)
FROM (tables or views)
WHERE (table_join_or filter)
AND (table_join_or_filter)
AND (table_join_or_filter)
ORDER BY (column_name_or_column_position);
```

```
SELECT (SELECT 'N' FROM DUAL) || (SELECT 'ew Y' FROM DUAL) || (SELECT 'ork ' FROM dual) || 'OUG' AS RESULT
FROM (SELECT 'DUAL' FROM dual)
WHERE (SELECT 1 FROM dual) = (SELECT 1 FROM dual)
AND (SELECT 2 FROM dual) BETWEEN (SELECT 1 FROM dual) AND (SELECT 3 FROM dual)
AND NVL((SELECT NULL FROM dual), (SELECT 'z' FROM dual)) = (SELECT 'z' FROM dual)
ORDER BY (SELECT 1 FROM dual);
```

UTL_INADDR

Execute on UTL_INADDR is Granted to PUBLIC (1:5)

- It takes precisely this much PL/SQL to attack

```
SQL> select utl_inaddr.get_host_address('www.umn.edu') from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UMN.EDU')
-----
134.84.119.107

SQL> select utl_inaddr.get_host_name('134.84.119.025') from dual;

UTL_INADDR.GET_HOST_NAME('134.84.119.025')
-----
g-smtp-w.tc.umn.edu
```

```
DECLARE
  h_name VARCHAR2(60);
  test_ip VARCHAR2(12) := '134.84.119.';
  suffixn NUMBER(3) := 0;
  suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```

Execute on UTL_INADDR is Granted to PUBLIC (2:5)

■ The output

```
134.84.119.001 - x-134-84-119-1.tc.umn.edu
134.84.119.002 - x-134-84-119-2.tc.umn.edu
134.84.119.003 - x-134-84-119-3.tc.umn.edu
134.84.119.004 - x-134-84-119-4.tc.umn.edu
134.84.119.005 - lsv-dd.tc.umn.edu
134.84.119.006 - mta-w2.tc.umn.edu
134.84.119.007 - isrv-w.tc.umn.edu
134.84.119.010 - mta-a2.tc.umn.edu
134.84.119.011 - x-134-84-119-9.tc.umn.edu
134.84.119.012 - x-134-84-119-10.tc.umn.edu
134.84.119.013 - x-134-84-119-11.tc.umn.edu
134.84.119.014 - x-134-84-119-12.tc.umn.edu
134.84.119.015 - x-134-84-119-13.tc.umn.edu
134.84.119.016 - x-134-84-119-14.tc.umn.edu
134.84.119.017 - diamond.tc.umn.edu
134.84.119.020 - x-134-84-119-16.tc.umn.edu
134.84.119.021 - oamethyst.tc.umn.edu
134.84.119.022 - x-134-84-119-18.tc.umn.edu
134.84.119.023 - x-134-84-119-19.tc.umn.edu
134.84.119.024 - vs-w.tc.umn.edu
134.84.119.025 - g-smtp-w.tc.umn.edu
134.84.119.026 - mta-w1.tc.umn.edu
134.84.119.027 - x-134-84-119-23.tc.umn.edu
134.84.119.030 - x-134-84-119-24.tc.umn.edu
134.84.119.031 - x-134-84-119-25.tc.umn.edu
134.84.119.032 - x-134-84-119-26.tc.umn.edu
134.84.119.033 - x-134-84-119-27.tc.umn.edu
134.84.119.034 - x-134-84-119-28.tc.umn.edu
134.84.119.035 - mon-w.tc.umn.edu
134.84.119.036 - ldapauth-w.tc.umn.edu
134.84.119.037 - ldap-w.tc.umn.edu
134.84.119.040 - mta-w3.tc.umn.edu
134.84.119.041 - x-134-84-119-33.tc.umn.edu
```

```
134.84.119.042 - x-134-84-119-34.tc.umn.edu
134.84.119.043 - smtp-w2.tc.umn.edu
134.84.119.044 - relay-w2.tc.umn.edu
134.84.119.045 - x-134-84-119-37.tc.umn.edu
134.84.119.046 - x-134-84-119-38.tc.umn.edu
134.84.119.047 - x-134-84-119-39.tc.umn.edu
134.84.119.050 - x-134-84-119-40.tc.umn.edu
134.84.119.051 - x-134-84-119-41.tc.umn.edu
134.84.119.052 - x-134-84-119-42.tc.umn.edu
134.84.119.053 - x-134-84-119-43.tc.umn.edu
134.84.119.054 - x-134-84-119-44.tc.umn.edu
134.84.119.055 - lsv-w.tc.umn.edu
134.84.119.056 - x-134-84-119-46.tc.umn.edu
134.84.119.057 - lists.umn.edu
134.84.119.060 - x-134-84-119-48.tc.umn.edu
134.84.119.061 - plaza.tc.umn.edu
134.84.119.062 - x-134-84-119-50.tc.umn.edu
134.84.119.063 - x-134-84-119-51.tc.umn.edu
134.84.119.064 - x-134-84-119-52.tc.umn.edu
134.84.119.065 - x-134-84-119-53.tc.umn.edu
134.84.119.066 - x-134-84-119-54.tc.umn.edu
134.84.119.067 - x-134-84-119-55.tc.umn.edu
134.84.119.070 - x-134-84-119-56.tc.umn.edu
134.84.119.071 - x-134-84-119-57.tc.umn.edu
134.84.119.072 - x-134-84-119-58.tc.umn.edu
134.84.119.073 - x-134-84-119-59.tc.umn.edu
134.84.119.074 - isrv-d2.tc.umn.edu
134.84.119.075 - ldapauth-d2.tc.umn.edu.tc.umn.edu
134.84.119.076 - ldap-d2.tc.umn.edu.tc.umn.edu
134.84.119.077 - x-134-84-119-63.tc.umn.edu
134.84.119.100 - x-134-84-119-100.tc.umn.edu
134.84.119.101 - aquamarine.tc.umn.edu
134.84.119.102 - x-134-84-119-102.tc.umn.edu
134.84.119.103 - x-134-84-119-103.tc.umn.edu
```

```
134.84.119.104 - mon-m.tc.umn.edu
134.84.119.105 - mta-m2.tc.umn.edu
134.84.119.106 - x-134-84-119-106.tc.umn.edu
134.84.119.107 - isrv-m.tc.umn.edu
134.84.119.108 - mta-m4.tc.umn.edu
134.84.119.109 - x-134-84-119-109.tc.umn.edu
134.84.119.110 - x-134-84-119-110.tc.umn.edu
134.84.119.111 - x-134-84-119-111.tc.umn.edu
134.84.119.112 - x-134-84-119-112.tc.umn.edu
134.84.119.113 - x-134-84-119-113.tc.umn.edu
134.84.119.114 - oaqua.tc.umn.edu
134.84.119.115 - x-134-84-119-115.tc.umn.edu
134.84.119.116 - x-134-84-119-116.tc.umn.edu
134.84.119.117 - x-134-84-119-117.tc.umn.edu
134.84.119.118 - x-134-84-119-118.tc.umn.edu
134.84.119.119 - x-134-84-119-119.tc.umn.edu
134.84.119.120 - vs-m.tc.umn.edu
134.84.119.121 - g-smtp-m.tc.umn.edu
134.84.119.122 - mta-m1.tc.umn.edu
134.84.119.123 - x-134-84-119-123.tc.umn.edu
134.84.119.124 - x-134-84-119-124.tc.umn.edu
134.84.119.125 - x-134-84-119-125.tc.umn.edu
134.84.119.126 - g-smtp-m4.tc.umn.edu
134.84.119.127 - x-134-84-119-127.tc.umn.edu
134.84.119.128 - x-134-84-119-128.tc.umn.edu
134.84.119.129 - x-134-84-119-129.tc.umn.edu
134.84.119.130 - ldapauth-m.tc.umn.edu
134.84.119.131 - ldap-m.tc.umn.edu
134.84.119.132 - mta-m3.tc.umn.edu
134.84.119.133 - x-134-84-119-133.tc.umn.edu
134.84.119.134 - x-134-84-119-134.tc.umn.edu
134.84.119.135 - smtp-m2.tc.umn.edu
134.84.119.136 - relay-m2.tc.umn.edu
134.84.119.137 - x-134-84-119-137.tc.umn.edu
```

- Let's go after the University of Utah instead

```
SQL> select utl_inaddr.get_host_address('www.utah.edu') from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UTAH.EDU')
-----
155.97.137.55

SQL> select utl_inaddr.get_host_name('155.97.137.045') from dual;

UTL_INADDR.GET_HOST_NAME('155.97.137.45')
-----
test.sys.utah.edu
```

```
DECLARE
  h_name VARCHAR2(60);
  test_ip VARCHAR2(12) := '155.97.137.';
  suffixn NUMBER(3) := 0;
  suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```

Execute on UTL_INADDR is Granted to PUBLIC (4:5)

- Attacked from a hotel room using public internet

```
155.97.136.006 - avaya-cms.vs.utah.edu
155.97.136.110 - dbw1.it.utah.edu
155.97.136.111 - sql-om.it.utah.edu
155.97.136.112 - sql-cm.it.utah.edu
155.97.136.113 - sql-bes.it.utah.edu
155.97.136.117 - dbw23.it.utah.edu
155.97.136.140 - d-ad.addev.utah.edu
155.97.136.141 - d-hsc.hscdev.addev.utah.edu
155.97.136.147 - d-mim.addev.utah.edu
155.97.136.148 - d-adfs.addev.utah.edu
155.97.136.149 - fim.addev.utah.edu
155.97.136.150 - d-ars.addev.utah.edu
155.97.136.153 - d-adlds.addev.utah.edu
155.97.136.157 - d-candes.addev.utah.edu
155.97.136.200 - b3.ddi.utah.edu
```

```
155.97.137.007 - slb1-campus-ddc-i11.net.utah.edu
155.97.137.010 - slb2-campus-ddc-j11.net.utah.edu
155.97.137.011 - slb-campus-ddc-vip.net.utah.edu
155.97.137.012 - slb3-campus-ddc-i11.net.utah.edu
155.97.137.021 - astra.utah.edu
155.97.137.022 - dars.sys.utah.edu
155.97.137.024 - webct.utah.edu
155.97.137.025 - jira.acs.utah.edu
155.97.137.026 - webctold.utah.edu
155.97.137.027 - stage.exchange.utah.edu
155.97.137.031 - my.utah.edu
155.97.137.032 - onboard.utah.edu
155.97.137.033 - uguest.utah.edu
155.97.137.034 - mytest.utah.edu
155.97.137.035 - campusmasterplan.utah.edu
155.97.137.036 - autodiscover.coe.utah.edu
```

```
155.97.137.040 - appdb.it.utah.edu
155.97.137.041 - gsa.search.utah.edu
155.97.137.043 - mrte.cc.utah.edu
155.97.137.044 - unite.utah.edu
155.97.137.045 - test.sys.utah.edu
155.97.137.046 - smtp.o365.umail.utah.edu
155.97.137.047 - vip-ipo.cc.utah.edu
155.97.137.050 - ipohsc.utah.edu
155.97.137.051 - staging.egi.utah.edu
155.97.137.052 - smtp.utah.edu
155.97.137.053 - ipo-forward.cc.utah.edu
155.97.137.054 - webstats8.utah.edu
155.97.137.055 - sdc8.utah.edu
155.97.137.060 - eq.utah.edu
155.97.137.061 - blocku.acs.utah.edu
155.97.137.062 - csmssl1.test.utah.edu
155.97.137.063 - sharepoint.it.utah.edu
155.97.137.066 - uitapp.it.utah.edu
155.97.137.067 - test.www.utah.edu
155.97.137.071 - ezproxy.test.utah.edu
155.97.137.072 - internalhub.umail.utah.edu
155.97.137.074 - legacy.umail.utah.edu
155.97.137.077 - ldap.acs.utah.edu
155.97.137.100 - go.utah.edu
155.97.137.102 - testvip2.sys.utah.edu
155.97.137.103 - ulogin.utah.edu
155.97.137.104 - jira.sys.utah.edu
155.97.137.105 - exc-sentry.med.utah.edu
155.97.137.106 - people.utah.edu
155.97.137.107 - www.test.utah.edu
```

```
155.97.137.109 - idp.idm.utah.edu
155.97.137.110 - gis-reporting.fm.utah.edu
155.97.137.114 - training.identity.utah.edu
155.97.137.118 - templates.utah.edu
155.97.137.150 - umailx.umail.utah.edu
155.97.137.223 - ese.idm.utah.edu
155.97.137.229 - test.go.utah.edu
155.97.137.232 - jira.test.utah.edu
155.97.137.234 - d-pki.addev.utah.edu
155.97.137.236 - gatetest.acs.utah.edu
155.97.137.237 - gatedev.acs.utah.edu
```

Execute on UTL_INADDR is Granted to PUBLIC (5:5)

- Attacked from a chair in the lobby here at Oracle in NYC public internet

156.110.247.001 - pharmacy.ouhsc.edu
156.110.247.002 - pcms.ouhsc.edu
156.110.247.003 - media.pharmacy.ouhsc.edu
156.110.247.004 - d212.ou.edu
156.110.247.005 - cba.ou.edu
156.110.247.006 - gradweb.ou.edu
156.110.247.007 - csold.ouhsc.edu
156.110.247.010 - new-minerva.ou.edu
156.110.247.011 - learn.eteam.ou.edu
156.110.247.012 - avp.ou.edu
156.110.247.013 - aperio.ouhsc.edu
156.110.247.014 - hippocrates.ouhsc.edu
156.110.247.015 - kentucky.ou.edu
156.110.247.016 - oup-cloverleaf.ouhsc.edu
156.110.247.017 - healthyhearts.ouhsc.edu
156.110.247.020 - pharmacyeval.ouhsc.edu
156.110.247.022 - csj.ou.edu
156.110.247.023 - pinnacle-prd.ou.edu
156.110.247.024 - new-myhousingandfood.ou.edu
156.110.247.025 - clsoffice.ou.edu
156.110.247.026 - sync.ouhsc.edu
156.110.247.027 - sync.ou.edu
156.110.247.030 - itservices.ouhsc.edu
156.110.247.031 - itservices.ou.edu
156.110.247.033 - colsw.ou.edu
156.110.247.034 - new-dn.ou.edu
156.110.247.035 - sis.ou.edu
156.110.247.036 - s2inb.ou.edu
156.110.247.037 - s2ssb.ou.edu
156.110.247.040 - sharepoint.ou.edu
156.110.247.041 - owa.ou.edu
156.110.247.042 - sis-poc.ou.edu
156.110.247.044 - clshelp.ou.edu

156.110.247.045 - s2cognos.ou.edu
156.110.247.046 - new-itsc.ou.edu
156.110.247.047 - sisapps.ou.edu
156.110.247.050 - pinnacle.ouhsc.edu
156.110.247.051 - oumed-csvr1.ouphysicians.com
156.110.247.052 - oumed-csvr2.ouphysicians.com
156.110.247.053 - oumed-telnet.ouphysicians.com
156.110.247.054 - wjec.ou.edu
156.110.247.055 - devcitrix.ouphysicians.com
156.110.247.056 - ozone-test.ou.edu
156.110.247.057 - pinnacletest.ouhsc.edu
156.110.247.060 - nor-poc-check.ou.edu
156.110.247.062 - oupharmacyleadership.org
156.110.247.063 - cki.ou.edu
156.110.247.064 - needhelp.ou.edu
156.110.247.065 - itc.ou.edu
156.110.247.066 - new-s3apps-uat.ou.edu
156.110.247.067 - ourm.ouphysicians.com
156.110.247.070 - new-check.ou.edu
156.110.247.071 - new-ozone1.ou.edu
156.110.247.072 - new-ozone.ou.edu
156.110.247.073 - iristest.ouhsc.edu
156.110.247.074 - new-webapps.ou.edu
156.110.247.075 - new-rdg.ou.edu
156.110.247.076 - eprint-new.ou.edu
156.110.247.077 - s3apps-new.ou.edu
156.110.247.100 - campuswebdev.ouhsc.edu
156.110.247.101 - intranet.nursing.ouhsc.edu
156.110.247.103 - wifi.ou.edu
156.110.247.105 - okautism.org
156.110.247.106 - devgecb.ouphysicians.com
156.110.247.107 - director.ouphysicians.com

156.110.247.109 - testpol.ouphysicians.com
156.110.247.110 - fwi.ouhsc.edu
156.110.247.111 - mediasite-dev.ouhsc.edu
156.110.247.112 - mediasite-iisvid7.ouhsc.edu
156.110.247.114 - adminservexch-1.ou.edu
156.110.247.115 - s3apps-tst.ou.edu
156.110.247.116 - canvas-svc.ou.edu
156.110.247.117 - hnsc.ouhsc.edu
156.110.247.118 - cs.ouhsc.edu
156.110.247.119 - selfservesa.ouhsc.edu
156.110.247.120 - oumed.ouphysicians.com
156.110.247.121 - nastiest.ouhsc.edu
156.110.247.122 - nsc.ouhsc.edu
156.110.247.123 - shibclone.ou.edu
156.110.247.130 - evm-new.ouhsc.edu
156.110.247.133 - profiles.ouhsc.edu
156.110.247.134 - perfectforms.ou.edu
156.110.247.135 - contact.ou.edu
156.110.247.143 - issportaltest.ou.edu
156.110.247.145 - illiad.ouhsc.edu
156.110.247.146 - skypeedgel.oumedicine.com
156.110.247.152 - hrwebtest.ouhsc.edu
156.110.247.153 - apps.hr.ou.edu
156.110.247.154 - benefitsenrollment.ouhsc.edu
156.110.247.155 - oupsys.ouphysicians.com
156.110.247.156 - tech.ouphysicians.com
156.110.247.157 - remote.ouhsc.edu
156.110.247.158 - nor-prov-srs.ou.edu
156.110.247.159 - hippocrates2.ouhsc.edu
156.110.247.160 - profilesdev.ouhsc.edu
156.110.247.161 - illiad2.ouhsc.edu
156.110.247.170 - fsold.ouhsc.edu
156.110.247.171 - fsrennew.ouhsc.edu

- Attacked from a chair in the lobby here at Oracle in NYC public internet

```
156.110.247.176 - psrs.ouhsc.edu
156.110.247.177 - mpsrs.ouhsc.edu
156.110.247.181 - selfservesaold.ouhsc.edu
156.110.247.182 - bomgar.ou.edu
156.110.247.197 - servicesapps.ou.edu
156.110.247.198 - travel.ouhsc.edu
156.110.247.199 - hub2.docsynergy.com
156.110.247.202 - nor-rh-satellite6.ou.edu
156.110.247.203 - commserve-proxy.ou.edu
156.110.247.204 - parkingvalidations.ouhsc.edu
156.110.247.205 - nsc-out.ouhsc.edu
156.110.247.207 - viptest.ouhsc.edu
156.110.247.208 - api-tst.ou.edu
156.110.247.209 - id-eteam.ou.edu
156.110.247.210 - api.ou.edu
156.110.247.211 - psattach2.ouhsc.edu
156.110.247.212 - oud4me.com
156.110.247.213 - limes3.ouhsc.edu
156.110.247.214 - planet.ou.edu
156.110.247.215 - bb-ts-app2.ou.edu
156.110.247.216 - caremgt.ouhsc.edu
156.110.247.217 - oulearningspace.ouhsc.edu
156.110.247.218 - remote-syslog.ouhsc.edu
156.110.247.219 - devconnect.ouphysicians.com
156.110.247.220 - devhelp.ouphysicians.com
156.110.247.221 - devtech.ouphysicians.com
156.110.247.223 - dev-scheduler.ou.edu
156.110.247.224 - spo.ou.edu
156.110.247.225 - marquee.ou.edu
156.110.247.226 - opioid.odmhsas.ou.edu
156.110.247.227 - hscvoicemail.ouhsc.edu
156.110.247.228 - hscfax.ouhsc.edu
156.110.247.229 - velos-test.ouhsc.edu
```

```
156.110.247.233 - smpp.ouphysicians.com
156.110.247.234 - ldap.ou.edu
156.110.247.235 - api-systemsofcare.ou.edu
156.110.247.236 - boomi-dev.ou.edu
156.110.247.237 - openmanage.ou.edu
156.110.247.238 - ahv.ouhsc.edu
156.110.247.239 - eteam-dev.ou.edu
156.110.247.240 - meetingmgr.ouhsc.edu
156.110.247.241 - boomi-prod.ou.edu
156.110.247.242 - testoumed.ouphysicians.com
156.110.247.243 - oumeddev.oumedicine.com
156.110.247.244 - nursing-eval.ouhsc.edu
156.110.247.245 - ncircle.ouhsc.edu
156.110.247.246 - sft.ouhsc.edu
156.110.247.250 - testvip.ouhsc.edu
156.110.247.254 - ns1.ouhsc.edu
```

How Comfortable Do You Feel About Your Perimeter Defense?

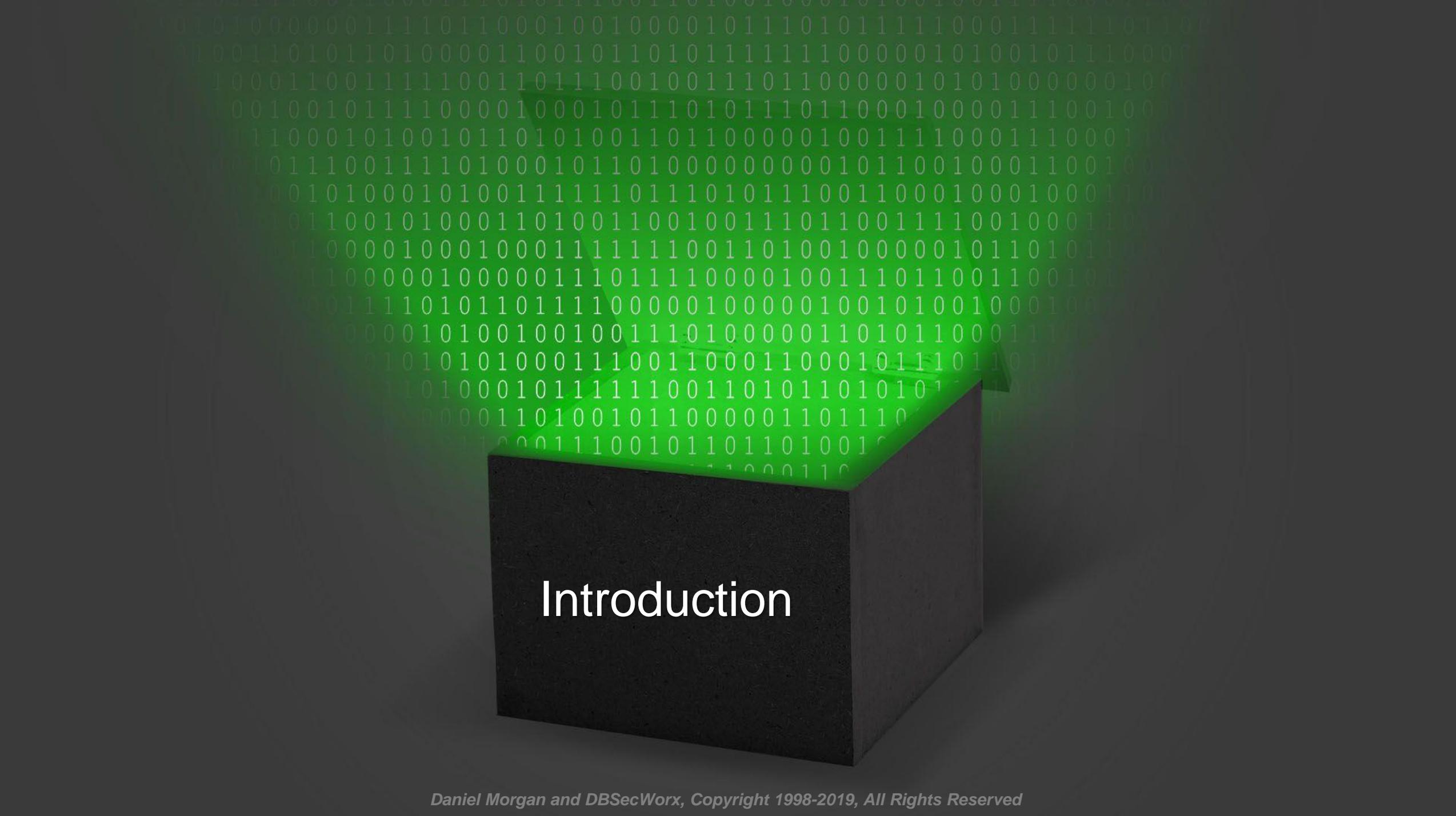
- Want to see what's visible from a Hilton Garden Inn in Bothell WA?

```
-- sample of 56 exposed IPs
130.76.32.044 - blv-crp-02.boeing.com
130.76.32.045 - blv-cbpn-02.boeing.com
130.76.32.051 - blv-csrp-04a.boeing.com
130.76.32.052 - blv-sec-cert-rp.boeing.com
130.76.32.053 - blv-vn-03.boeing.com
130.76.32.054 - blv-vabsd.esddh.boeing.com
130.76.32.055 - blv-smdac.esddh.boeing.com
130.76.32.072 - ciemftstelift1.boeing.com
130.76.32.073 - blv-psxms1-01.boeing.com
130.76.32.074 - ciemftste2ift1.boeing.com
130.76.32.075 - dhcp17a.boeing.com
130.76.32.077 - ciemftstelift2.boeing.com
130.76.32.103 - bcag-fwal-01.boeing.com
130.76.32.106 - igx33-03-12bb5-a.boeing.com
130.76.32.108 - igx33-03-12bb5-c.boeing.com
130.76.32.112 - blv-mbf-01.boeing.com
130.76.32.113 - nt-ops-12.beds.boeing.com
130.76.32.116 - blv-sw-01.boeing.com
130.76.32.244 - blv-prprd.esddh.boeing.com
```

```
-- all 19 exposed IPs
130.76.184.016 - gtmx50-115-a.boeing.com
130.76.184.101 - southwest1-pre.mobile.connect.boeing.com
130.76.184.106 - phxntpx1.ntp.boeing.net
130.76.184.107 - phxptp1.ntp.boeing.net
130.76.184.122 - cite-mbf.boeing.com
130.76.184.123 - cite-bpn.boeing.com
130.76.184.124 - cite-cert-bpn.boeing.com
130.76.184.138 - www-prd-12.exi.boeing.com
130.76.184.139 - www-prd-13.exi.boeing.com
130.76.184.158 - southwest2.connect.boeing.com
130.76.184.170 - phx-mbsin-01.mbs.boeing.net
130.76.184.171 - phx-mbsin-02.mbs.boeing.net
130.76.184.172 - phx-mbsin-03.mbs.boeing.net
130.76.184.173 - phx-mbsin-04.mbs.boeing.net
130.76.184.178 - phx-mbsout-01.mbs.boeing.net
130.76.184.179 - phx-mbsout-02.mbs.boeing.net
130.76.184.212 - phxdnsxp01.dns.boeing.net
130.76.184.217 - phxdnsxr01.dns.boeing.net
130.76.184.222 - phxdnsexnr01.dns.boeing.net
```

- Want to guess what "sec-cert" is?
- How about "dhcp17a"?
- What is "bcag-fwal-01"? ... I bet it is a firewall at Boeing Commercial Airplane Group
- What are the odds that every server at Boeing in Phoenix is connected to NTP and DNS?





Introduction



- 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 Users Group
- damorgan@dbsecworx.com



System/370-145 system console

www.morganslibrary.org



Morgan's Library

www library

Search

International Oracle Events 2016-2017 Calendar

Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct

The Library

The library is a spam-free on-line resource with code demos for DBAs and Developers. If you would like to see new Oracle database functionality added to the library ... just email us. Oracle Database 12cR2 is now available in the Cloud. If you are not already working in a 12cR1 CDB database ... you are late to the party and you are losing your competitive edge.

Home

Resources

- Library
- How Can I?
- Presentations
- Links
- Book Reviews
- Downloads
- User Groups
- Blog
- Humor

General

- Contact
- About
- Services
- Legal Notice & Terms of Use
- Privacy Statement

Presentations Map



Mad Dog Morgan



Training Events and Travels

- OTN APAC, Sydney, Australia - Oct 31
- OTN APAC, Gold Coast, Australia - Nov 02
- OTN APAC, Beijing China - Nov 04-05
- OTN APAC, Shanghai China - Nov 06
- Sangam16, Bangalore, India - Nov 11-12
- NYOUG, New York City - Dec 07

Next Event: Indiana Oracle Users Group

Oracle Events



Click on the map to find an event near you

Morgan



aboard USA-71



Library News

- Morgan's Blog
- Morgan's Oracle Podcast
- US Govt. Mil. STIGs (Security Checklists)
- Bryn Llewellyn's PL/SQL White Paper
- Bryn Llewellyn's Editing White Paper
- Explain Plan White Paper



ACE News

Would you like to become an Oracle ACE?

Learn more about becoming an ACE



- ACE Directory
- ACE Google Map
- ACE Program
- Stanley's Blog

This site is maintained by Dan Morgan. Last Updated: 11/08/2016 22:25:14

This site is protected by copyright and trademark laws under U.S. and International law. © 1998-2016 Daniel A. Morgan All Rights Reserved

ORACLE OTN Oracle Mix Share Twitter Facebook Library Contact Us Privacy Statement Legal Notices & Terms of Use

www.dbsecworx.org

DBSecWorx

 Search

www library

Home

Products

Services

Resources

Community

Relationships

Company

If everyone had access to your networks ... but could not access your data ... what would be at risk?

If you deployed every security product on your wish list would your databases be secure?

DBSecWorx secures data and databases

Learn How We Do It

[Blog](#)

[Principles](#)

[Principals](#)

[Contact Us](#)

Copyright © 2019 DBSecWorx All rights reserved.

[Privacy & Cookies Policy](#)

[Privacy Shield](#)

[Legal](#)



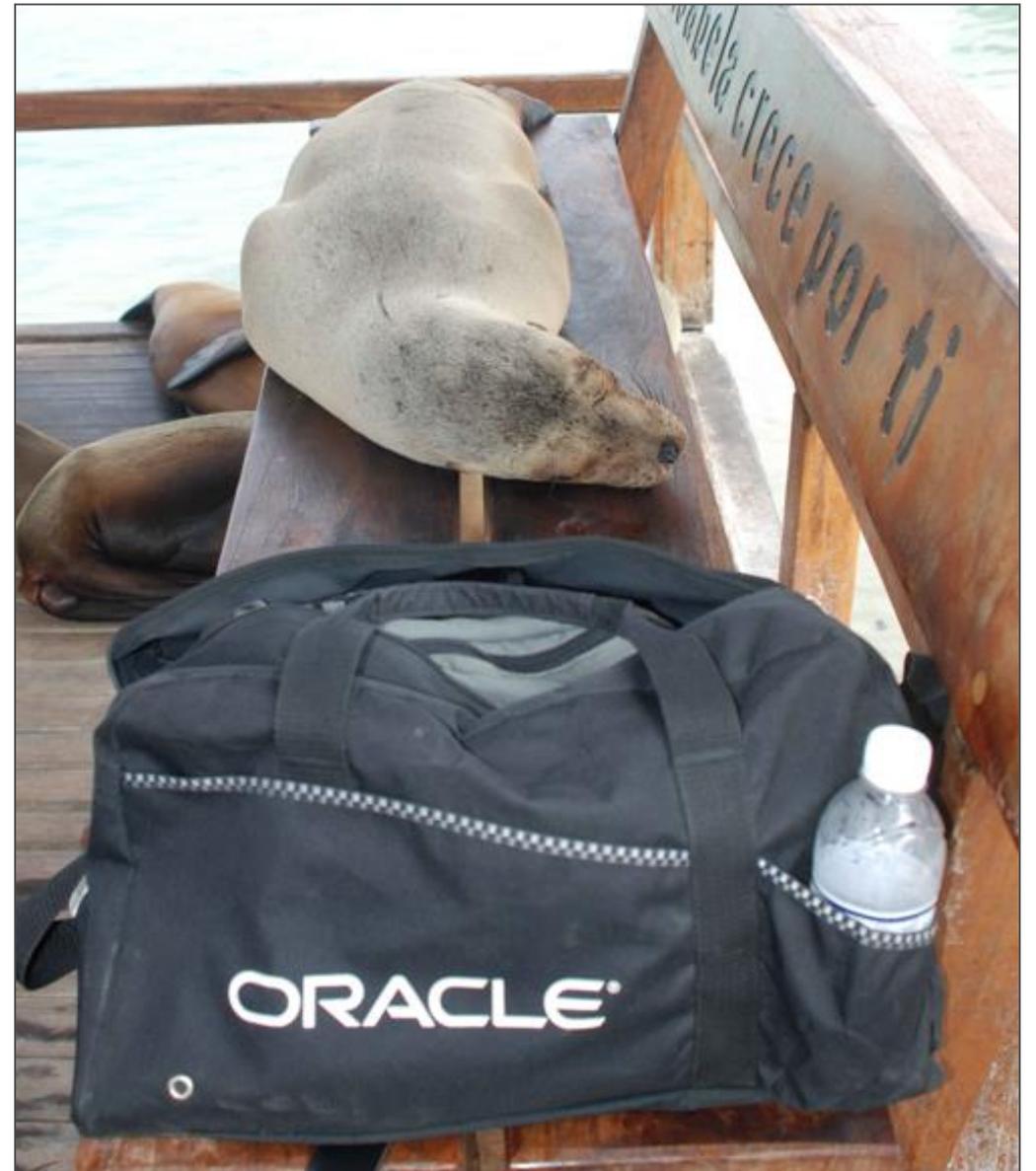
To get to the gate where my plane was waiting I had to go through a metal detector and luggage inspection. Good thing I wasn't carrying beard scissors because they would have been confiscated.

Lucky me though, once I got to business class they provided me with the means to defend myself against those brutes back in coach.

Air travel is a lot like IT security ... most of the focus is on the perimeter.



Travel Log: Galapagos Islands, Ecuador 2014



- 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.

- If 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 will explain what happened after your mortgage payment bounces
- Auditing, after the damage is already done, tells you what you wouldn't have lost if you had focused your efforts on improving security
- Auditing, Compliance, and Governance do not provide security



Where We Are

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."

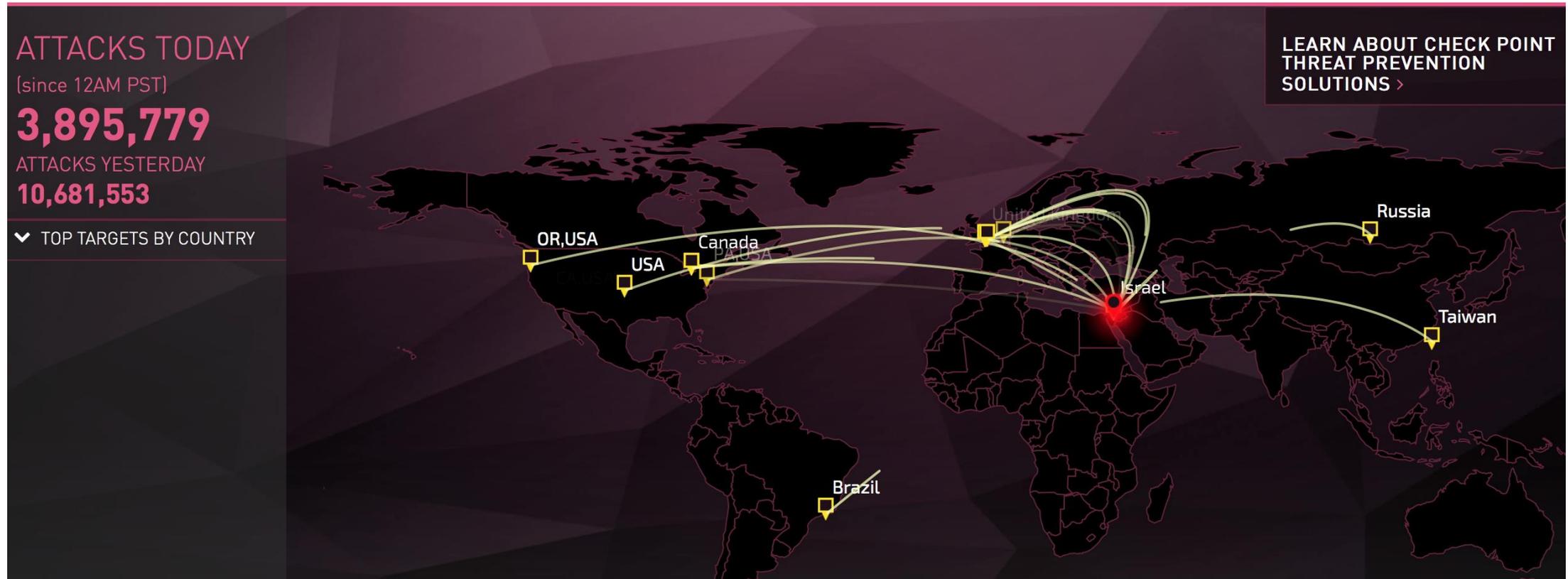
JIM SALTER - 2/25/2019, 6:30 AM

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 just looked 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

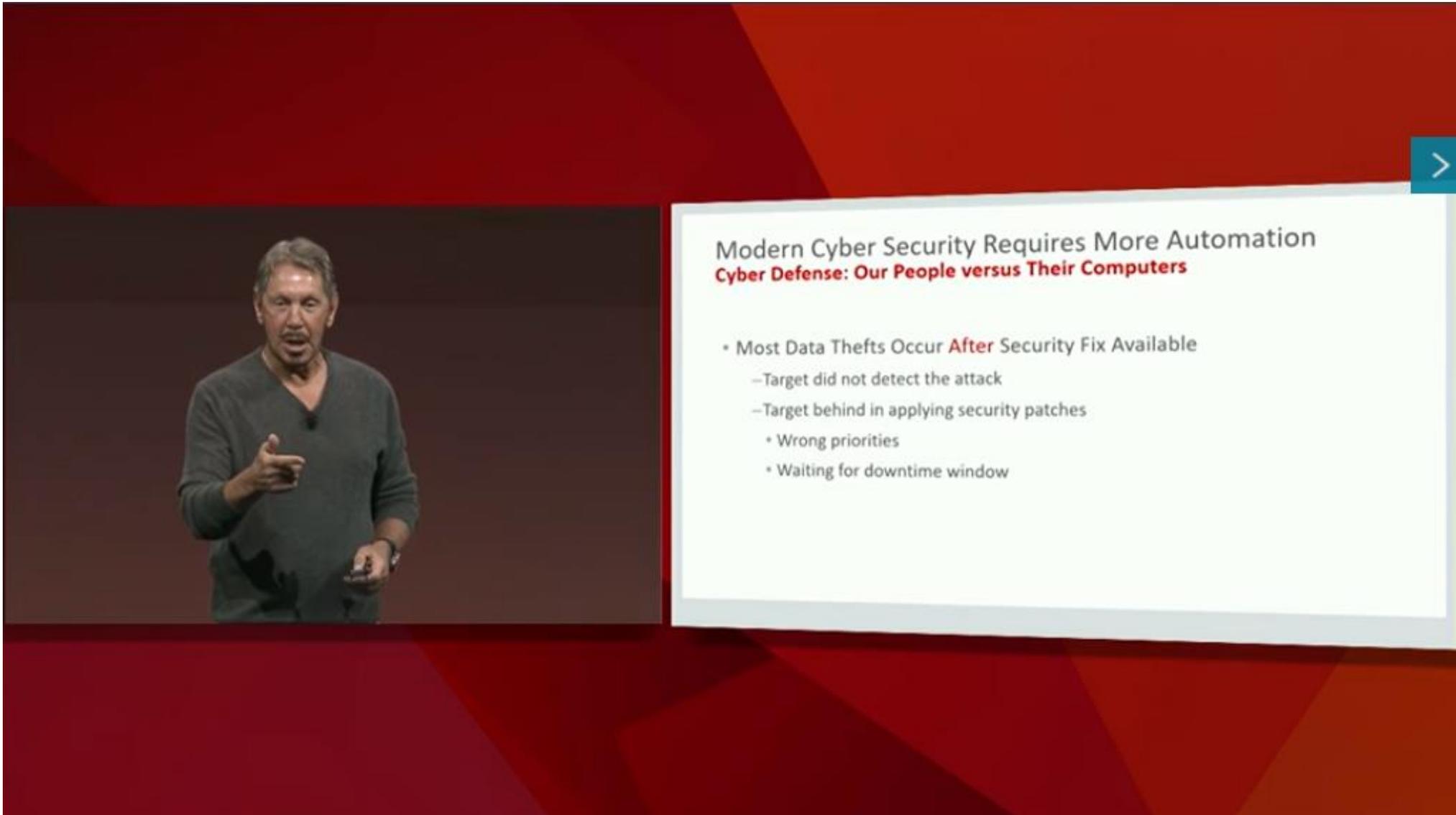
- Most databases break-ins are never detected and never reported
- What you hear about is the part of the iceberg above the water
- Database related risks fall into three broad categories
 - Data Theft
 - Data Alteration
 - Transforming the database into an attack tool
- To accomplish these activities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





Cyber Attacks: More Data Stolen Every Year
Cyber Criminals and State Actors are Winning the Cyber War

- Equifax: Records of 143,000,000 Americans plus...
 - Credit Card Numbers, Social Security Numbers, home addresses...
 - Equifax CEO, executives and IT management team resigns
- Office of Personnel Management: Records of 20 Million Federal Employees
 - Security clearance data, finger print data, social security numbers, home addresses
 - White House, Foreign Embassies, State Department, Defense Department...
 - Director of OPM Resigns
- Cyber Criminals and **State Actors** steal more data every year
 - Formidable and sophisticated adversaries stealing corporate & government data



>

Modern Cyber Security Requires More Automation

Cyber Defense: Our People versus Their Computers

- Most Data Thefts Occur **After** Security Fix Available
 - Target did not detect the attack
 - Target behind in applying security patches
 - Wrong priorities
 - Waiting for downtime window

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?

The screenshot shows the OPM.gov website's Cybersecurity Resource Center. At the top, there is a navigation bar with links for Morgan's Library, Google, Email, Humor, News, Oracle, SciTech, and TidalScale. Below this is the OPM.GOV logo and a main navigation menu with links for ABOUT, POLICY, INSURANCE, RETIREMENT, SUITABILITY, AGENCY SERVICES, and NEWS. The breadcrumb trail indicates the current location: OPM.gov Main > Cybersecurity Resource Center > Frequently Asked Questions. On the left side, there is a sidebar with a section titled 'IN THIS SECTION' containing links for Sign Up for Services, Cybersecurity Incidents, Recent Updates, Frequently Asked Questions (highlighted), and Stay Informed. Below the sidebar is a 'PRINT PAGE' button. The main content area features the title 'Cybersecurity Resource Center' and the sub-section 'FREQUENTLY ASKED QUESTIONS'. A paragraph explains that the section will be updated with answers to questions about incidents and the notification process. Below this are five dark grey buttons: 'What happened', 'About the impacted information', 'Who has been impacted', 'Getting notified if your data was compromised', and 'Protecting your identity'. At the bottom, there are three light blue expandable question cards, each with a plus icon and a question: 'What happened during the OPM cybersecurity incidents announced in 2015?', 'Who responded to these incidents?', and 'What was included in a background investigation file?'. A 'Safari' browser tab is visible at the bottom left.

+ 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

- 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 Tiffany's?
get a stereo system at Best Buy?
get an AmEx card?

What You Can Do

Here are steps you can take to protect your identity:

- + Spot the warning signs of identity theft
- + Be aware of phishing scams
- + Update your passwords
- + Get up to speed on computer security
- + If you think your identity has been stolen
- + Learn how to keep your information safe from exploitation
- + Tips for practicing safe online behavior every day

- Perhaps I like to live dangerously but for some reason I didn't consider it likely the PLA 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 had applied for a security clearance
- 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](#).

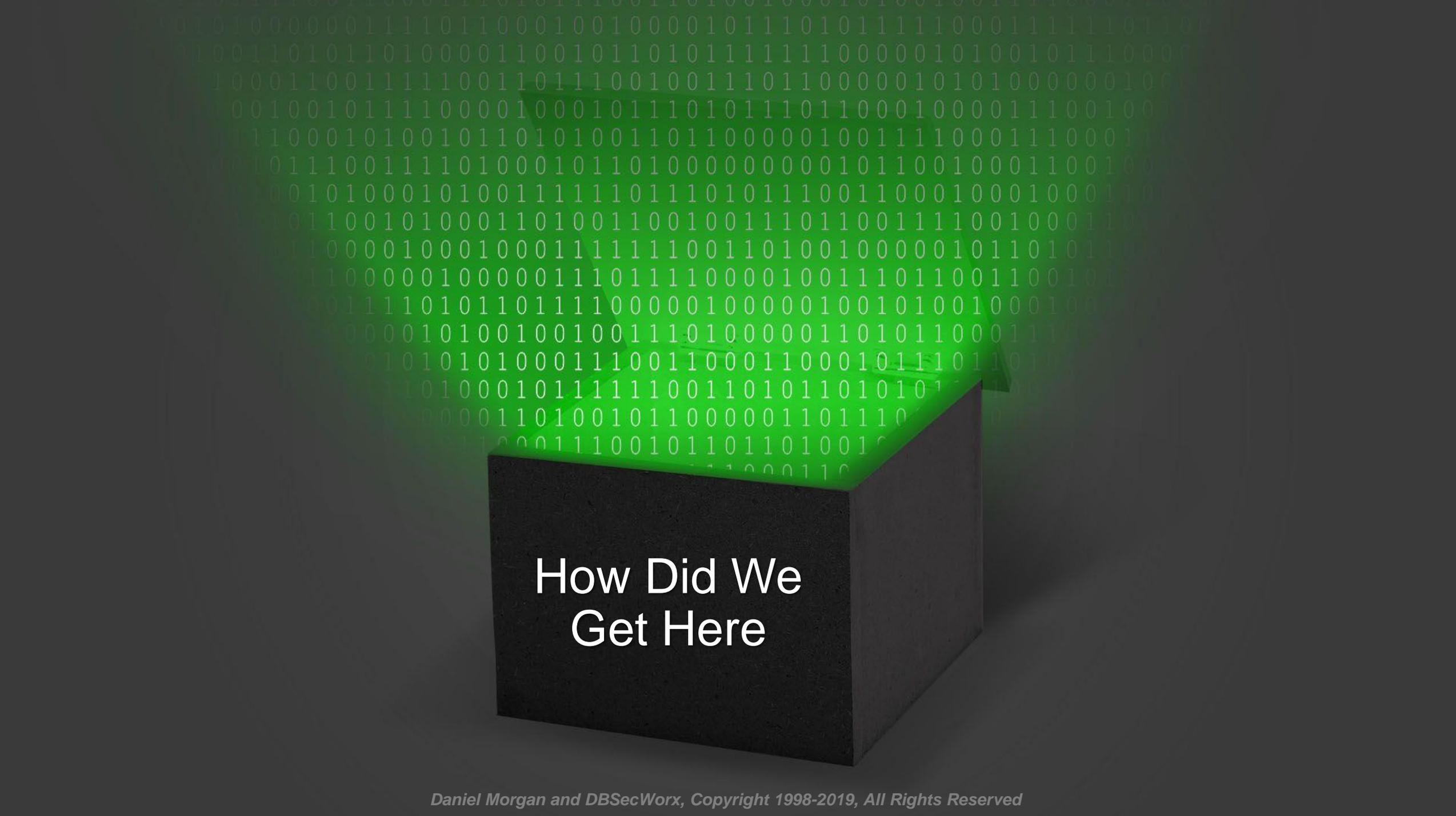
Instructions on how to enroll in other services were included in your notification. If you have not yet received a notification but believe you were impacted by the 2015 cybersecurity incidents please visit the [Verification Center](#) .

An Unpleasant Fact

- Governance is NOT security
- Auditing is NOT security
- Compliance is NOT security
- The overwhelming majority of encryption does not enhance 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 [company] were broken into, data on [###] billions of credit cards was stolen and the [company] failed to pass their compliance and security audits?
- You likely never will
- Victims of database breaches pass their audits ... proving audits and penetration tests are not the same as to securing data ... so what is?



How Did We Get Here

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



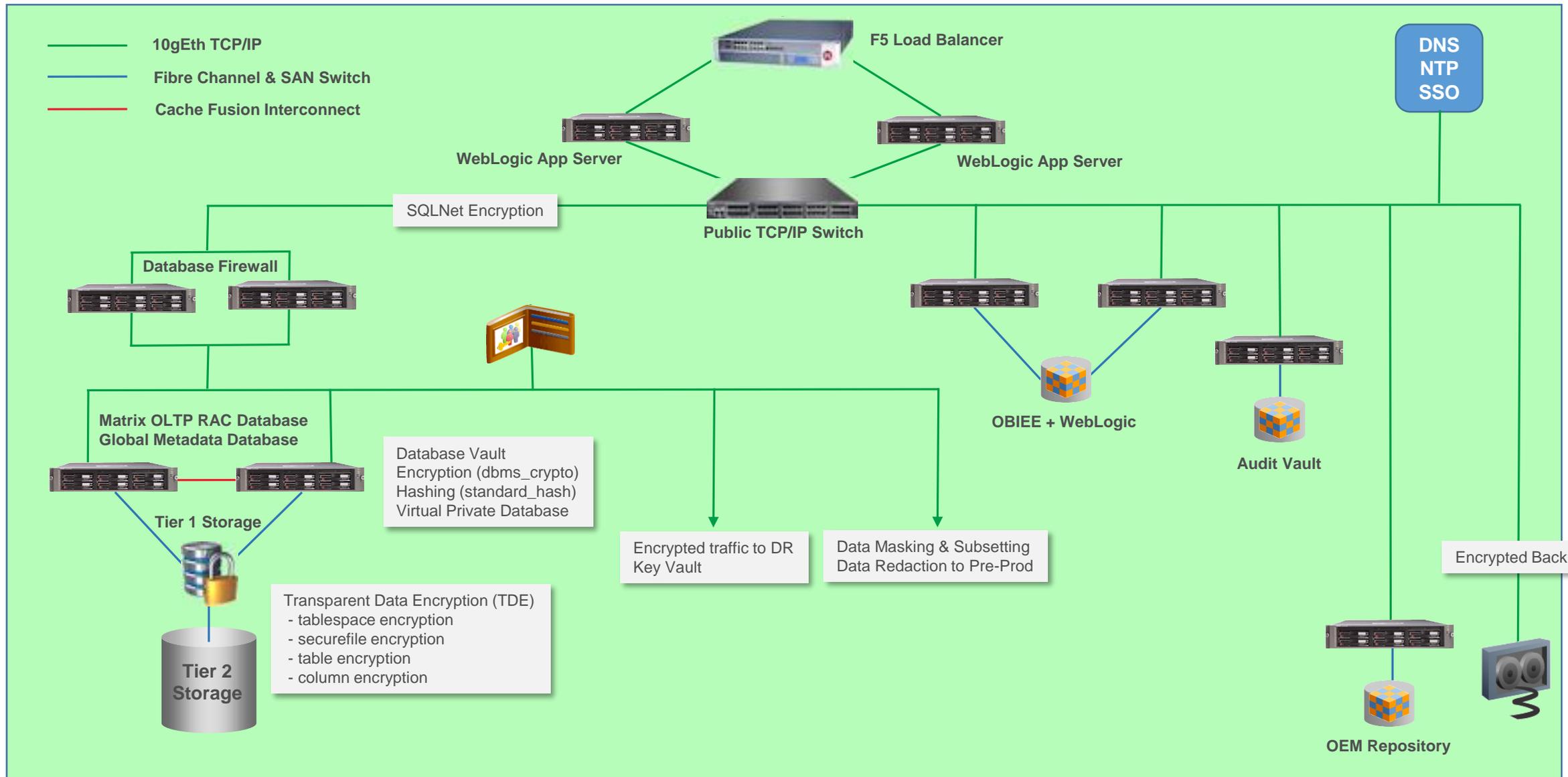
Hefin Richards

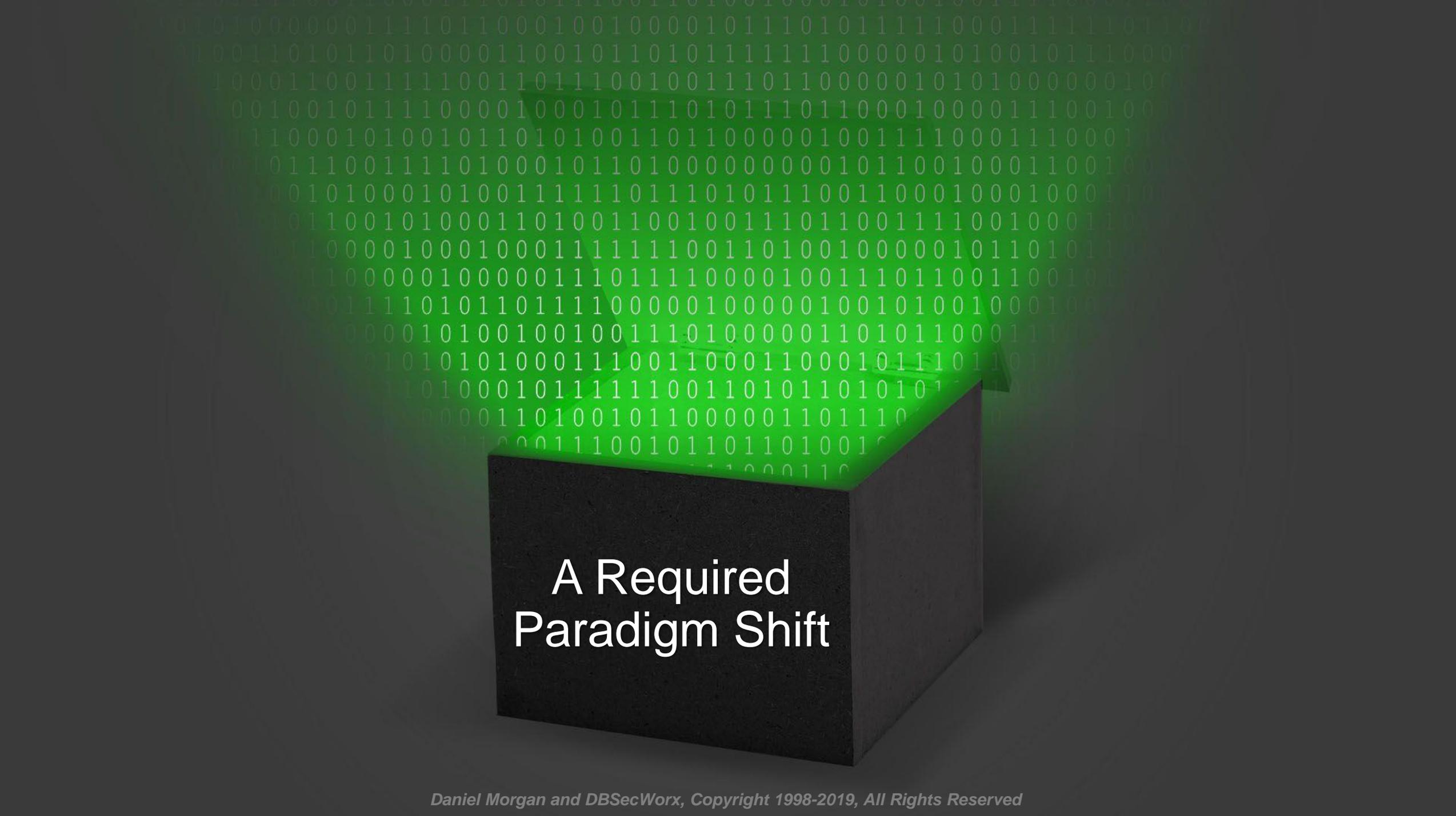
- Every Oracle Database deployment requires multiple network connections

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





A Required Paradigm Shift

Today: I Need To Change The Way You Think

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

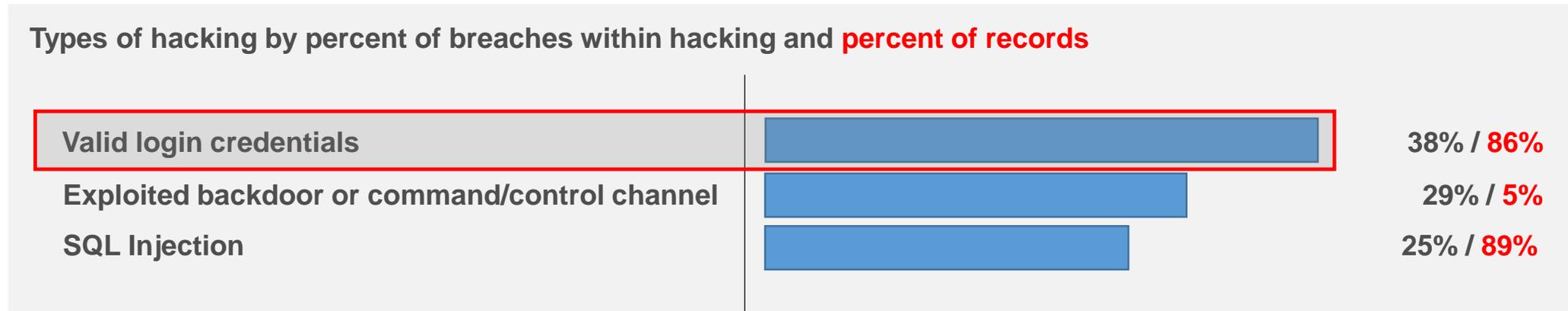
Pay Attention To What Should Have Been Said ... But Wasn't

- 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

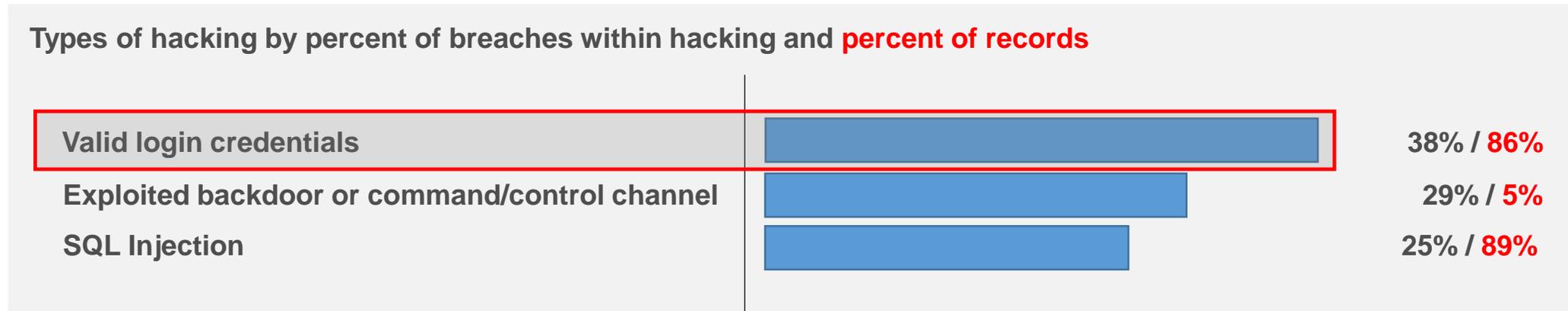


- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

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

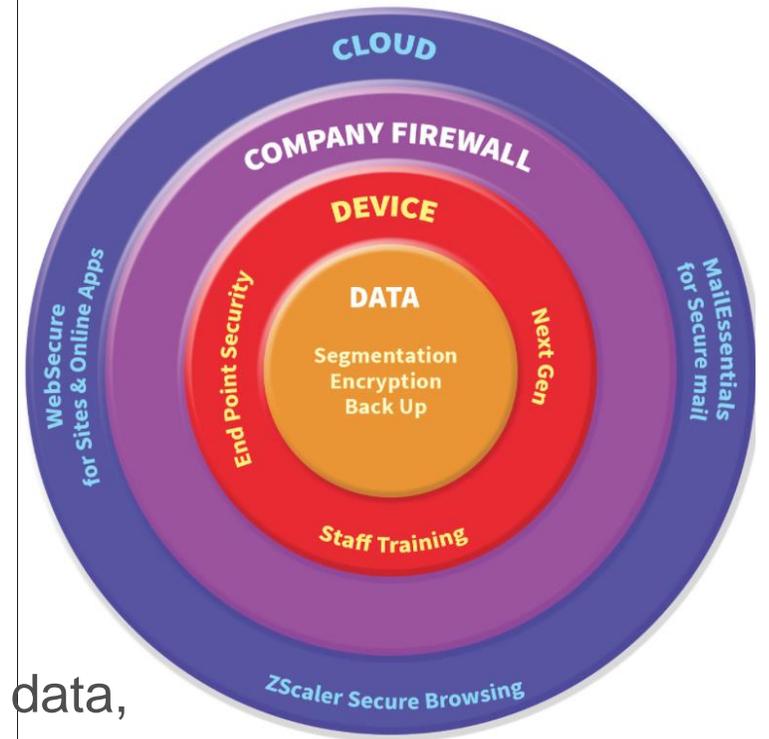
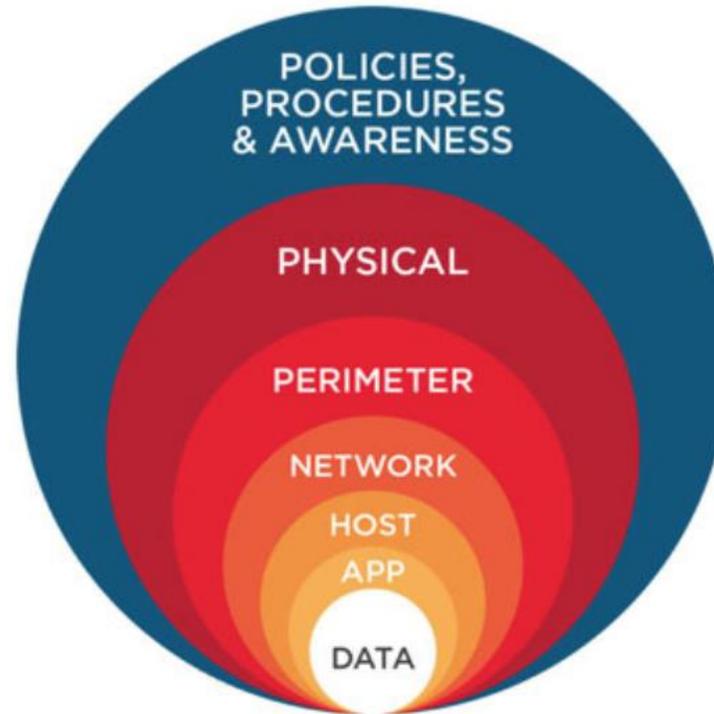
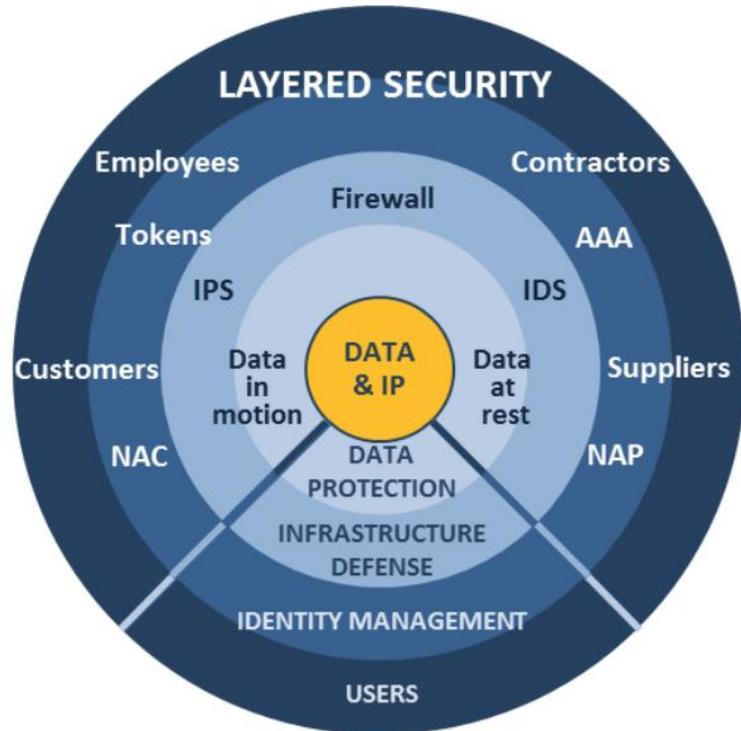
- Apply security patches immediately
- Stop using cron - use DBMS_SCHEDULER
- Change passwords regularly - automate the process
- Do not grant the CONNECT, RESOURCE, or DBA roles ever
- Use Proxy Users for every connecting user you create
- Implement Database Vault
- **Implement Row Level Security**

- 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



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

If everyone could penetrate the network but no one could get to the data ... you win

- 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



A 3D black cube is centered in the lower half of the image. The top surface of the cube is illuminated with a bright green glow. The background is a dark grey gradient with a pattern of faint, light green binary code (0s and 1s) scattered across it.

Wrap Up

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=hrrpd1
PRD_R_UNAME=rman_pshrprd
PRD_R_PWD=pspr0d11
PRD_BK=/backup/hrrpd/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
```



Our New Reality

- There isn't room in IT for Conscientious Objectors



Conclusion

- Success requires that we develop a new approach to our jobs
- That we reprioritize securing existing systems over creating new and insecure systems
- We must lead our employers to an understanding that passing audits is not sufficient
- We must stop implementing new feature before we understand the potential risks



Free Offer

- I am personally providing
- Oracle Database Security Lunch & Learns
- Targeted for IT management
or
- Targeted for IT technicians
- No Cost
- No Products To Sell
- No Sales Pitch

- If interested email me: damorgan@dbsecworx.com

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

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

