VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

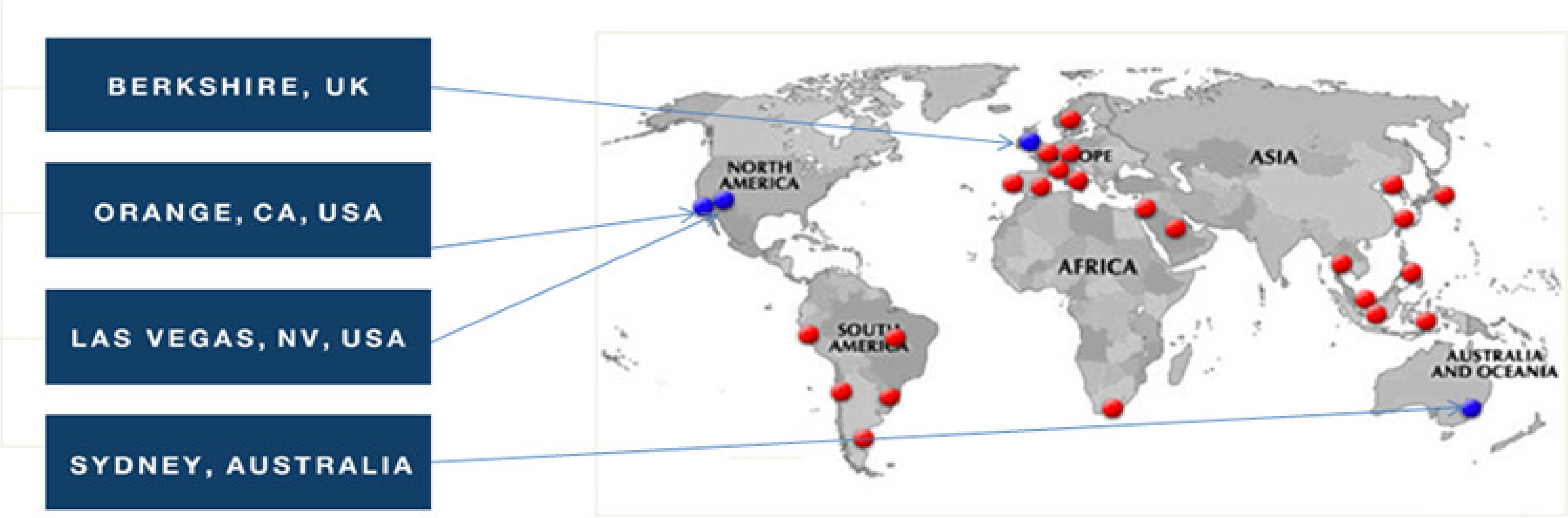
Top 5 Most Prevalent Assessment Findings

Brian Marshall
VP of Research and Development

About Vanguard

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Founded:	1986
Business:	Cybersecurity Experts for Large Enterprises Software, Professional Services, and Training
Customers:	1,000+ Worldwide


BERKSHIRE, UK

ORANGE, CA, USA

LAS VEGAS, NV, USA

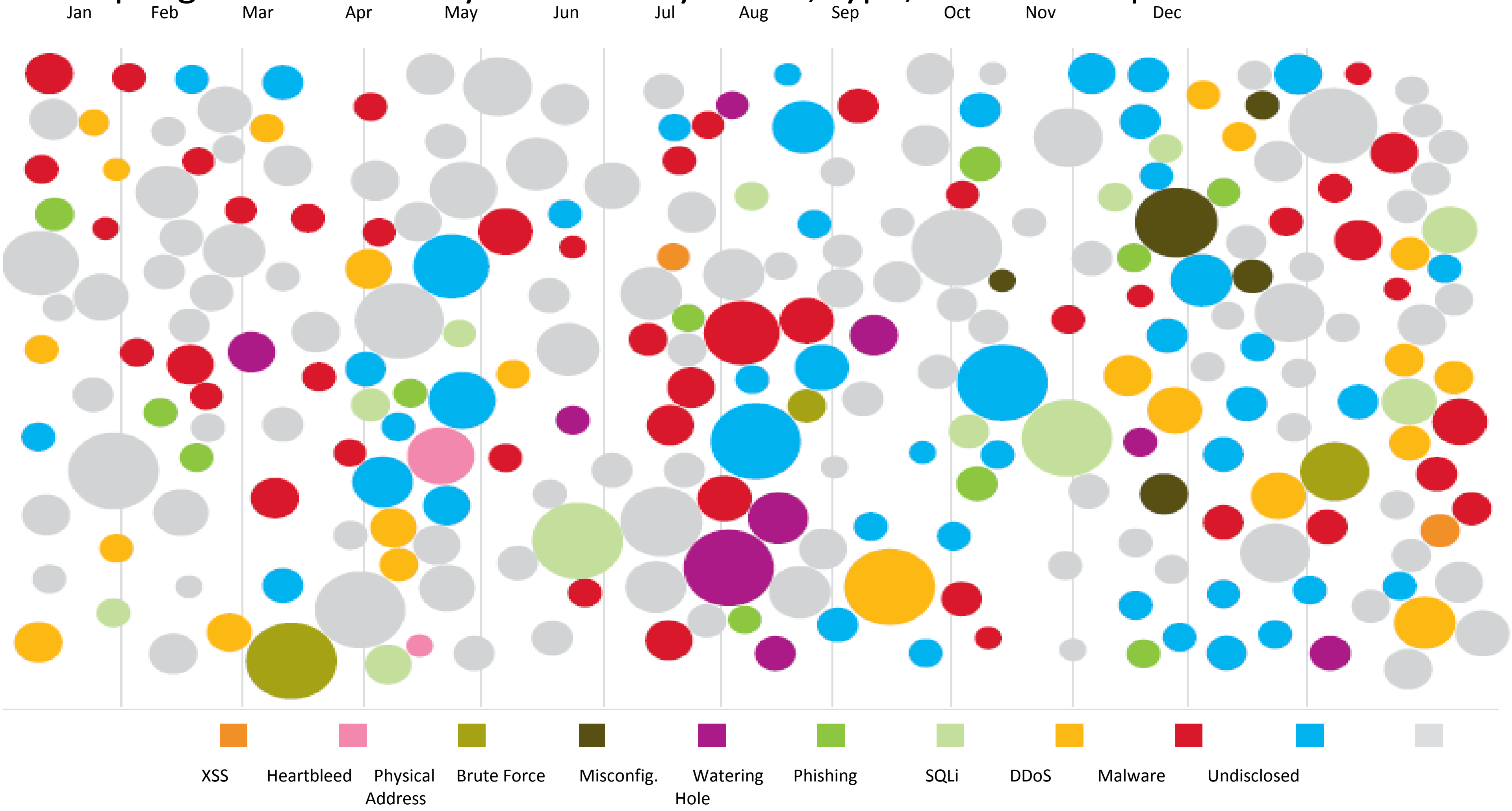
SYDNEY, AUSTRALIA

Over 15 distributors/resellers serving 50+ countries worldwide

ATTACK STATISTICS

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Sampling of 2014 security incidents by attack, type, time and impact



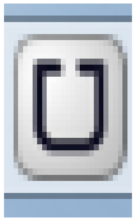
Source: IBM X-Force Threat Intelligence Quarterly, 1Q 2015

Top Recent Breaches

ebay

Anthem.

EMC²



JPMorganChase

THE HOME DEPOT

RSA

PREMERA | BLUE CROSS

IRS

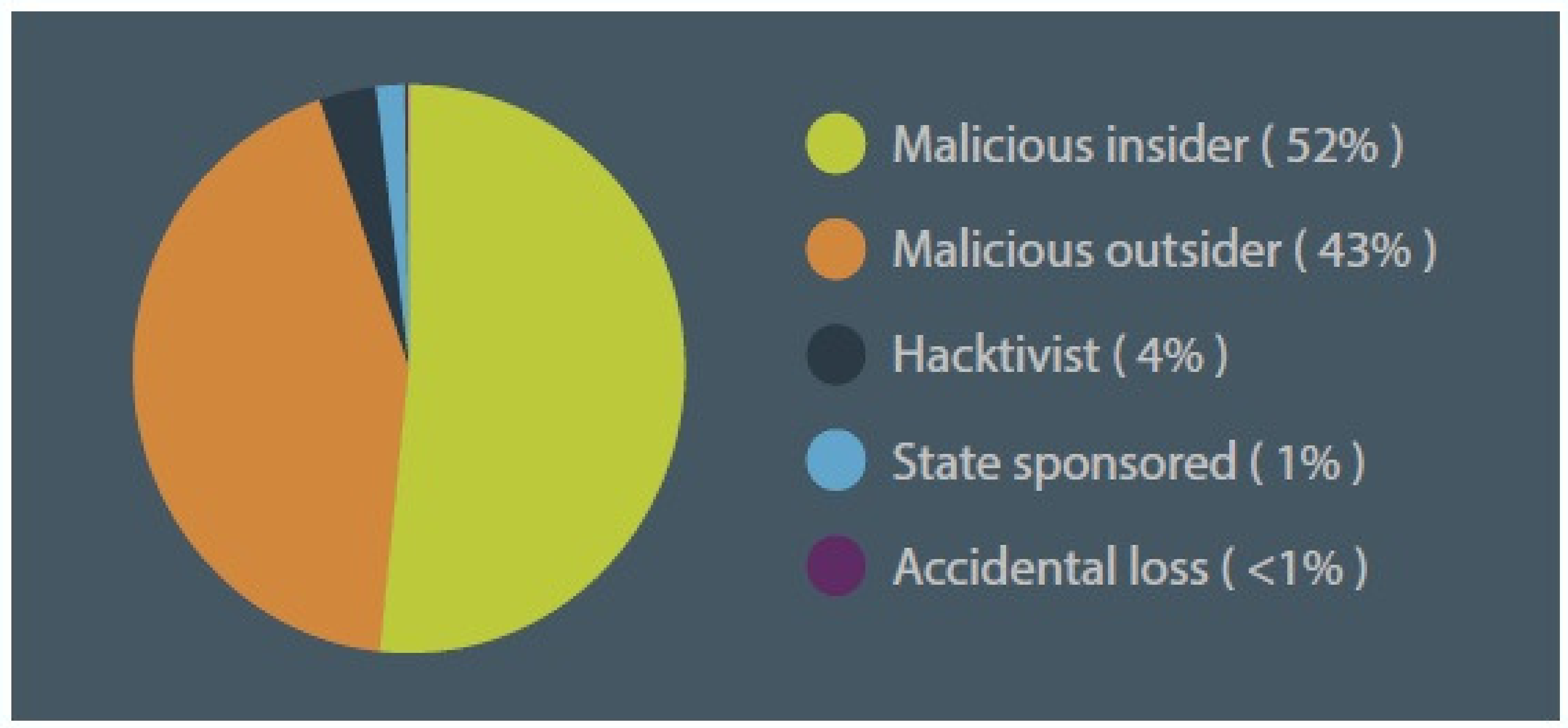
Michaels
Where Creativity Happens

SONY
PICTURES

Data Breaches

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

TOP BREACH RECORDS BY SOURCE



My Grandchildren

The Mainframe

ComputerWeekly.com

Mainframe at 50: Why the mainframe keeps on going

For the past 50 years, the mainframe has been the technological workhorse enabling go

In fact, 80% of the world's corporate data is still managed by mainframes.

In a video interview with Computer Weekly's Cliff Saran, IBM Hursley lab director Rob La computing paradigms and application systems, such as the move to the web and mobile technology.

"The platform is continually reinventing itself to remain relevant for cloud and mobile computing and to be able to run the most popular application server packages," he said.
Yet while it appears to be middle-aged technology, in terms of reach it seems the mainframe touches almost everything in modern life, according to Lamb.

“If you are using a mobile application today that runs a transactio is a four in five chance that there is a mainframe behind that tran

And the amount of processing run on the mainframe dwarfs the i 60,000 Google searches. But the CICs application server, which ru billion transactions a day," he said.

IBM will be formally celebrating the 50th anniversary of the Syste

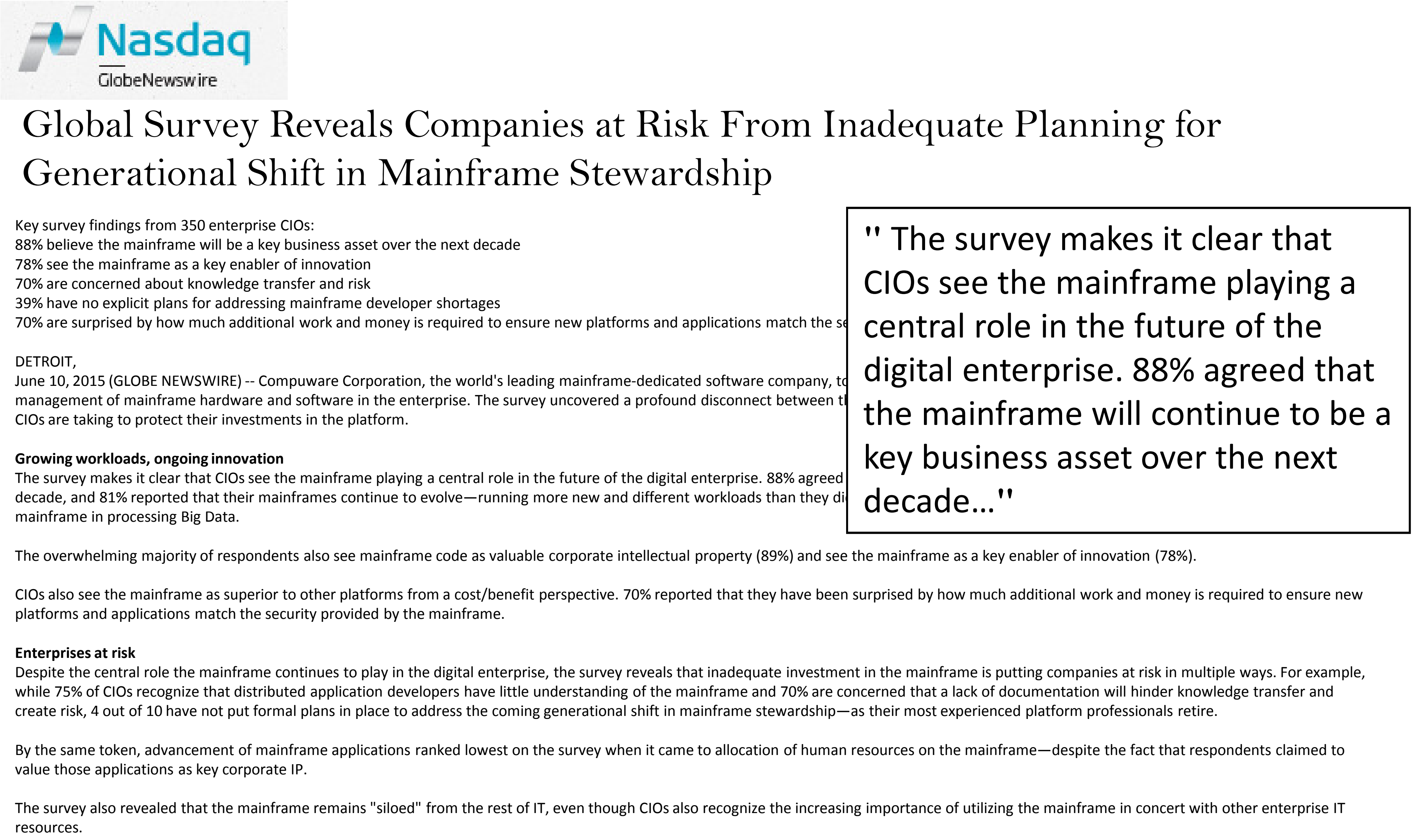
> " 80% of the world’s corporate data is still managed by mainframes."

> "If you are using a mobile application today that runs a transaction to check your bank balance or transfer money from one account to another, there is a four in five chance that there is a mainframe behind that transaction."

Source: Computer Weekly; Interview with Rob Lamb, IBM Hursley lab director, March 24, 2014

Survey of 350 CIO’s on the Mainframe

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Nasdaq
GlobeNewswire

Global Survey Reveals Companies at Risk From Inadequate Planning for Generational Shift in Mainframe Stewardship

Key survey findings from 350 enterprise CIOs:
88% believe the mainframe will be a key business asset over the next decade
78% see the mainframe as a key enabler of innovation
70% are concerned about knowledge transfer and risk
39% have no explicit plans for addressing mainframe developer shortages
70% are surprised by how much additional work and money is required to ensure new platforms and applications match the se

DETROIT,
June 10, 2015 (GLOBE NEWSWIRE) -- Compuware Corporation, the world's leading mainframe-dedicated software company, to
management of mainframe hardware and software in the enterprise. The survey uncovered a profound disconnect between th
CIOs are taking to protect their investments in the platform.

Growing workloads, ongoing innovation
The survey makes it clear that CIOs see the mainframe playing a central role in the future of the digital enterprise. 88% agreed
decade, and 81% reported that their mainframes continue to evolve—running more new and different workloads than they di
mainframe in processing Big Data.

The overwhelming majority of respondents also see mainframe code as valuable corporate intellectual property (89%) and see the mainframe as a key enabler of innovation (78%).

CIOs also see the mainframe as superior to other platforms from a cost/benefit perspective. 70% reported that they have been surprised by how much additional work and money is required to ensure new platforms and applications match the security provided by the mainframe.

Enterprises at risk
Despite the central role the mainframe continues to play in the digital enterprise, the survey reveals that inadequate investment in the mainframe is putting companies at risk in multiple ways. For example, while 75% of CIOs recognize that distributed application developers have little understanding of the mainframe and 70% are concerned that a lack of documentation will hinder knowledge transfer and create risk, 4 out of 10 have not put formal plans in place to address the coming generational shift in mainframe stewardship—as their most experienced platform professionals retire.

By the same token, advancement of mainframe applications ranked lowest on the survey when it came to allocation of human resources on the mainframe—despite the fact that respondents claimed to value those applications as key corporate IP.

The survey also revealed that the mainframe remains "siloed" from the rest of IT, even though CIOs also recognize the increasing importance of utilizing the mainframe in concert with other enterprise IT resources.

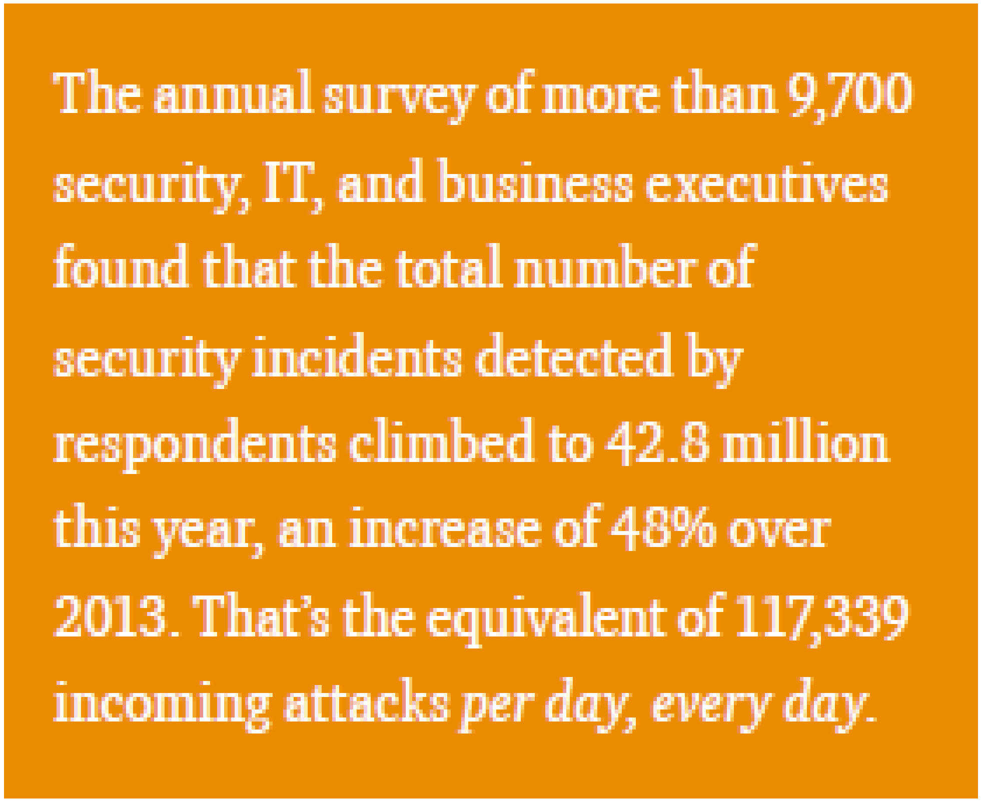
> " The survey makes it clear that CIOs see the mainframe playing a central role in the future of the digital enterprise. 88% agreed that the mainframe will continue to be a key business asset over the next decade…"

Source: Nasdaq GlobeNewswire, Compuware Corporation, June 10, 2015

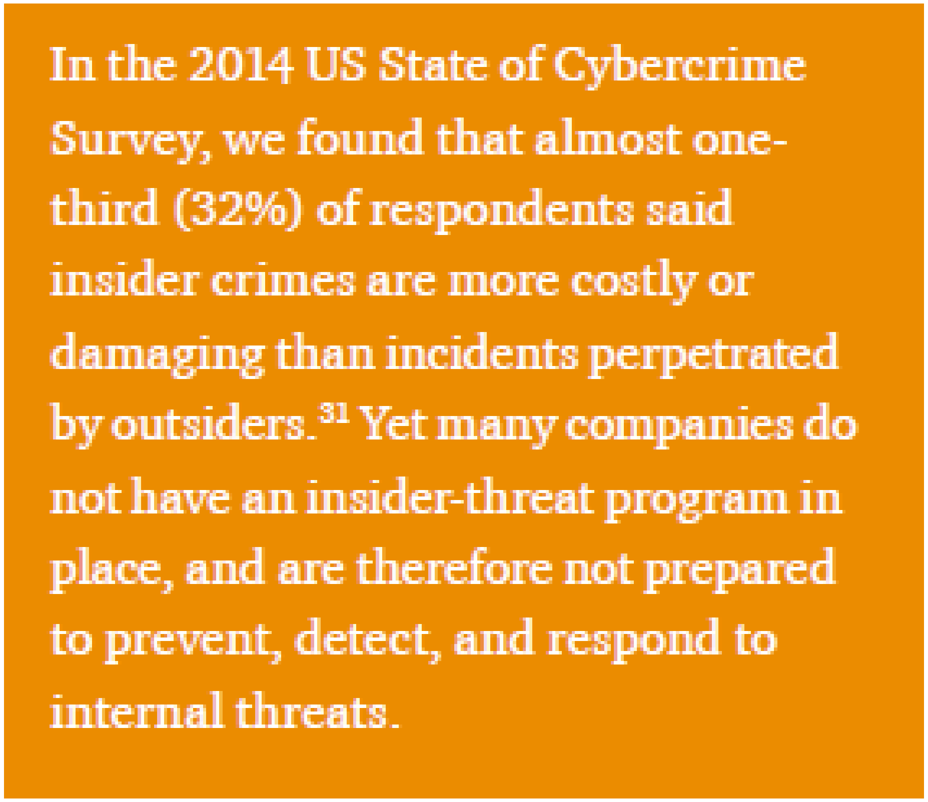
Managing cyber risks in an interconnected world

Key findings from The Global State of Information Security® Survey 2015

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



The annual survey of more than 9,700 security, IT, and business executives found that the total number of security incidents detected by respondents climbed to 42.8 million this year, an increase of 48% over 2013. That's the equivalent of 117,339 incoming attacks *per day, every day.*



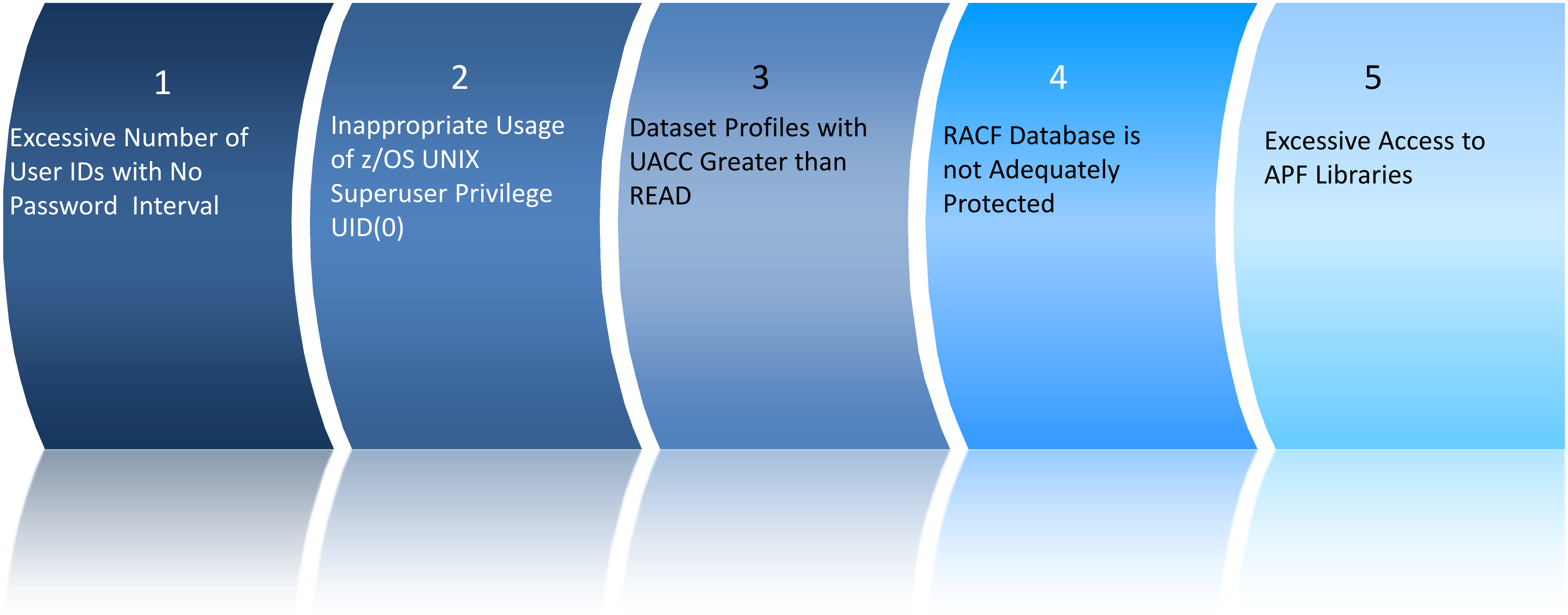
In the 2014 US State of Cybercrime Survey, we found that almost one-third (32%) of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders.[31] Yet many companies do not have an insider-threat program in place, and are therefore not prepared to prevent, detect, and respond to internal threats.

Source: PWC.COM, September 30, 2014

Vulnerability Assessment Findings

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Scope: Vanguard Top 5 z/OS Risks Identified in Client Security Assessments



1
Excessive Number of User IDs with No Password Interval

2
Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

3
Dataset Profiles with UACC Greater than READ

4
RACF Database is not Adequately Protected

5
Excessive Access to APF Libraries

Note: Data collected from hundreds of security assessments performed by Vanguard Integrity Professionals.

“Top Five” Assessment Finding #1

Finding	Excessive Number of User IDs with No Password
Explanation	User IDs with no password Interval are not required to change their passwords
Risk	Since passwords do not need to be changed periodically, people who knew a password for an ID could still access that ID even if they are no longer authorized users.
Remediation	Review each of the personal user profiles to determine why they require NOINTERVAL. Their passwords should adhere to the company policy regarding password changes. If the user ID is being used for started tasks or surrogate, it should be reviewed and changed to PROTECTED.

“Top Five” Assessment Finding #2

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Finding

Inappropriate Usage of z/OS UNIX Superuser Privilege, UID=0

Explanation

User IDs with z/OS UNIX superuser authority, UID(0), have full access to all UNIX directories and files and full authority to administer z/OS UNIX.

Risk

Since the UNIX environment is the z/OS portal for critical applications such as file transfers, Web applications, and TCPIP connectivity to the network in general, the ability of these superusers to accidentally or maliciously affect these operations is a serious threat. No personal user IDs should be defined with an OMVS segment specifying UID(0).

Remediation

The assignment of UID(0) authority should be minimized by managing superuser privileges by granting access to one or more of the ‘BPX.qualifier’ profiles in the FACILITY class and/or access to one or more profiles in the UNIXPRIV class.

“Top Five” Assessment Finding #3

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Finding

Dataset Profiles with UACC Greater than READ

Explanation

The UACC value for a dataset profile defines the default level of access to which any user whose user ID or a group to which it has been connected does not appear in the access list.

Risk

Data sets that are protected by a RACF profile with a UACC greater than READ allow most users with system access to read or modify these data sets. In addition, users may be able to delete any data set covered by the dataset profiles that have a UACC of ALTER.

Remediation

Review each of these profiles and determine whether the UACC is appropriate. For those profiles where the UACC is excessive, you will have to determine who really needs access before changing the UACC. To find out who is accessing these data sets, review SMF data to determine who is accessing the data sets with greater than READ access.

“Top Five” Assessment Finding #4

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Finding

RACF Database is not Adequately Protected

Explanation

The RACF database contains extremely sensitive security information. No access to the RACF database is required for normal administration activities using either RACF commands or the RACF provided ISPF panels.

Risk

Any user who has read access to the RACF database or any backup copy could make a copy and then use a cracker program to find passwords for user IDs and could obtain a list of user IDs and resources.

Remediation

Review the protection for the RACF database and any backup copies and remove any access list entries granting access higher than NONE, other than to senior RACF administrators and system staff tasked to run RACF database utilities.

“Top Ten” Assessment Finding #5

Finding

Excessive Access to APF Libraries

Explanation

Authorized Program Facility (APF) libraries are in integral part of the z/OS architecture to enable maintenance of the integrity of the z/OS operating system environment. Libraries designated as APF allow programs to execute with the authority of z/OS itself, so the ability to modify these libraries must be strictly controlled.

Risk

UPDATE or higher access to an APF library can allow an individual to create an authorized program which can bypass security controls and execute privileged instructions. UPDATE or higher access should be limited to senior systems support staff.

Remediation

Review the protection of all APF libraries and remove or change inappropriate access list entries and ensure that all UPDATE activity is logged to SMF.

Top Ten Critical Assessment Findings in Mainframe Environments

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

The percentage numbers represent the percentages of environments in which Vanguard has found this configuration error in over 190 environments in the last 8 years.

73%	Excessive Number of User ID's w/No Password Interval	SEVERE
60%	Inappropriate Usage of z/OS UNIX Superuser Privilege, UID = 0	SEVERE
53%	Data Set Profiles with UACC Greater than READ	SEVERE
41%	RACF Database is not Adequately Protected	SEVERE
40%	Excessive Access to APF Libraries	SEVERE
40%	General Resource Profiles in WARN Mode	SEVERE
34%	Dataset Profiles in WARN Mode	SEVERE
53%	Data Set Profiles with UACC of READ	HIGH
52%	Improper Use or Lack of UNIXPRIV Profiles	HIGH
51%	Started Task IDs are not Defined as PROTECTED IDs	HIGH

*Vanguard rates security configuration errors as:

SEVERE (needs immediate remediation)
HIGH (needs plan of remediation for some point in the relatively near future)
MEDIUM (needs plan of remediation for some point in the future)
LOW (should be remediated when time and resources permits)

Questions

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Thank You

Call us at 800-794-0014
or
email us at info@go2vanguard.com