جلوگیری از نشت داده

محمدرضا مهرآزما

محمدرضا مهرآزما

کارشناس ارشد فناوری اطلاعات – شبکه های کامپیوتری
مشاور رسمی فناوری اطلاعات
متخصص در حوزه امنیت اطلاعات
عضو رسمی کمیسیون افتا (امنیت فضای تبادل اطلاعات) نظام صنفی
عضو رسمی کمیسیون مشاوران نظام صنفی
مدرس دوره های امنیت

Related Certificates:

Charles Sturt University:

. Digital Forensics
. Applying Law to Emerging Cyber Dangers
. Cloud Models, Architecture, and Risk Management

TUV Rhineland and QMS Italy: ISMS Auditor/Lead Auditor ISO/IEC27001:2005

Avira: Technical Expert

Kaspersky Lab: Certified Professional

McAfee: Risk Advisor, Application Control, DLP, Firewall enterprise

Falcongaze: Secure Tower DLP Technical Support

راه های ارتباطی:
آدرس وب سایت: www.Mehrazma.com
ایمیل: Mehrazma@Mehrazma.com
تلگرام: @Mehrazma
لینکدین: https://ir.linkedin.com/in/mehrazma

مفاهیم اولیه

اهمیت دارایی های اطلاعاتی

جلوگیری از نشت اطلاعات

Data leakage Prevention

Data loss Prevention

سرقت اطلاعات شخصی در صدر شکایت ها قرار دارد

برای پنجمین سال متوالی دزدی اطلاعات در صدر شکایت ها قرار دارد.

بیش از ده میلیون سرقت اطلاعات در سال گزارش می شود.

۵۹ درصد شرکت ها رخدادهایی درداخل شبکه های خود شناسایی می کنند که هزینه ای بالغ بر ۵ میلیارد دلار برای مشتریان و ۴۸ میلیارد دلار برای شرکت ها ایجاد می نماید.

۵ درصد از اطلاعات برای اهداف تروریستی دزدیده شده اند.

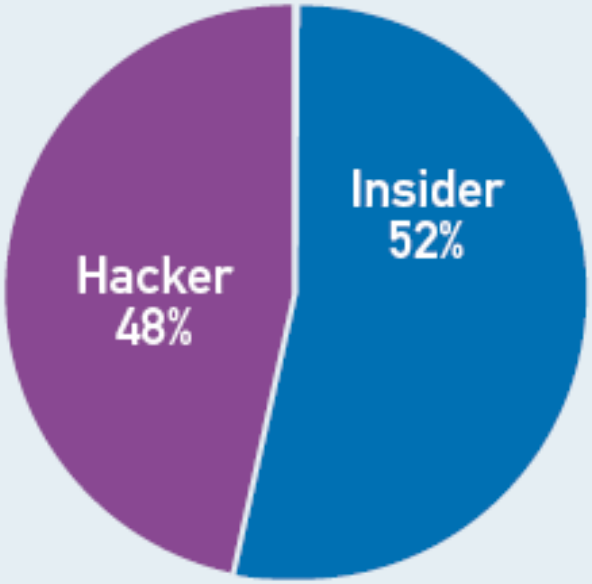
۱۵ درصد از اطلاعات برای مصارف جنایی دزدیده شده اند.

۱۵ درصد از اطلاعات برای گروه های مواد مخدر دزدیده شده اند.

بیش از ۲۳ ایالت در آمریکا در حال تهیه پیش نویس یا تایید قوانینی در این خصوص هستند.

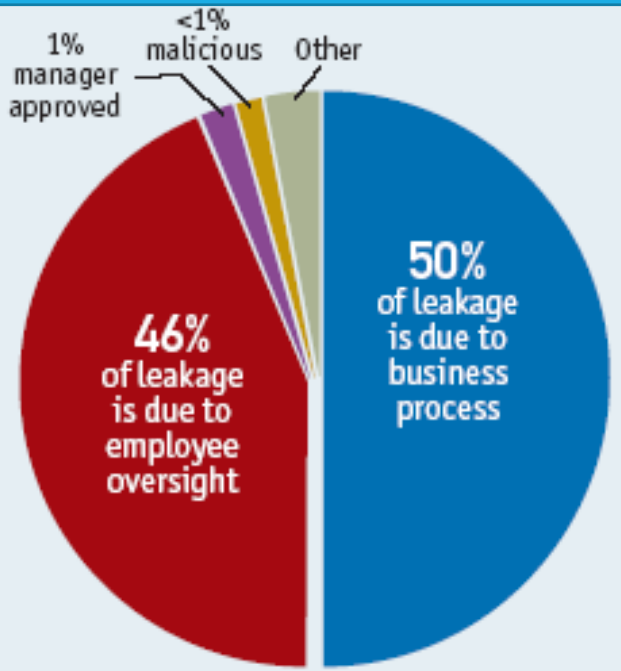
تغییر داده تهدیدی برای امنیت داده ها

تهدیدات داخلی در مقابل تهدیدات هکرها
تا سال های پیش امن کردن محیط در برابر هکرها اولین سیاست و اولویت امنیتی بود
که از سال ۲۰۰۵ به بعد تغییر کرد.

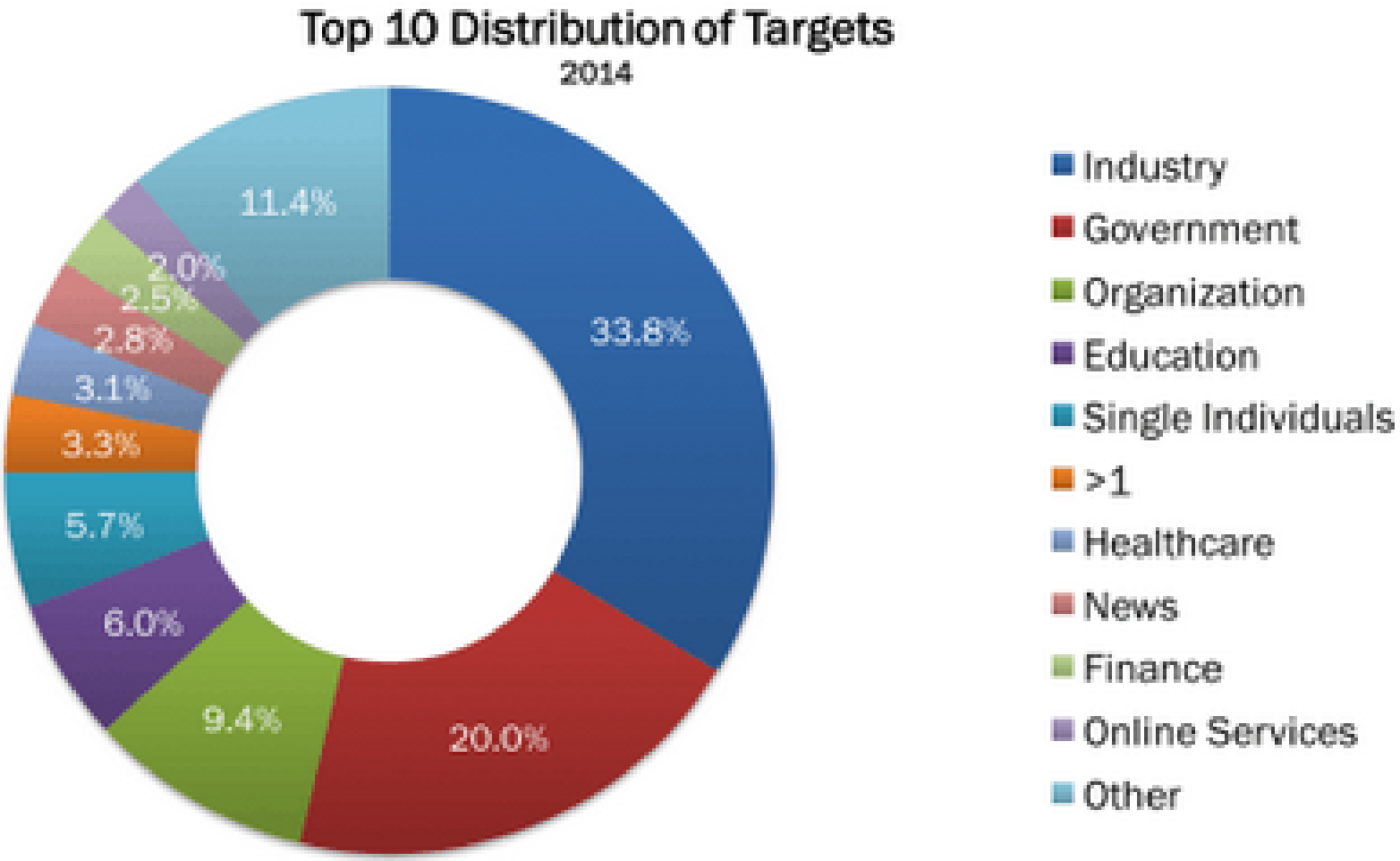


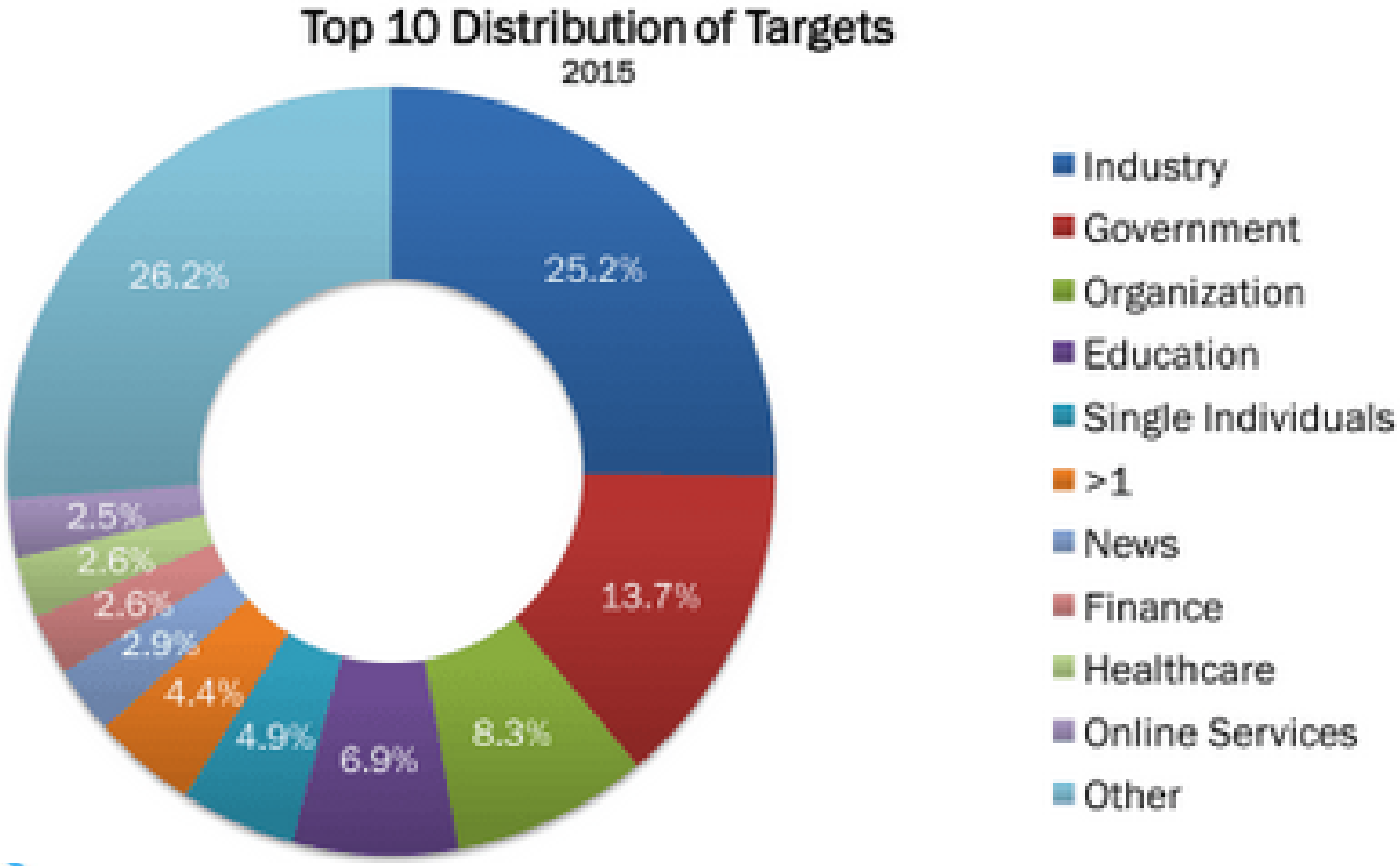
Data compiled from industry sources
including EPIC.org and PerkinsCoie.com.

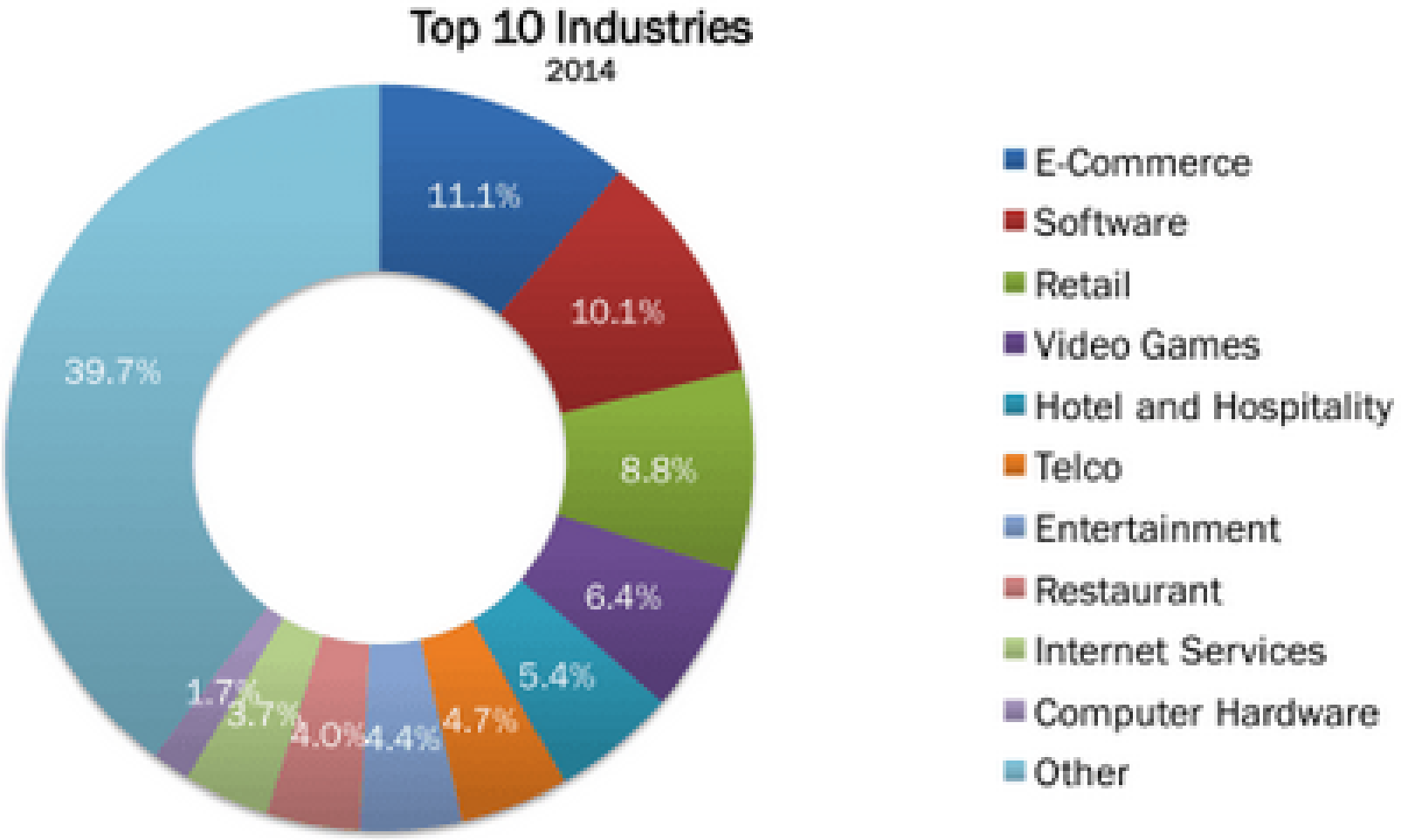
غیر عمدی در مقابل عمدی
۹۶ درصد نشت اطلاعات برای پردازش های اشتباه یا تحت نظارت اتفاق افتاده است.

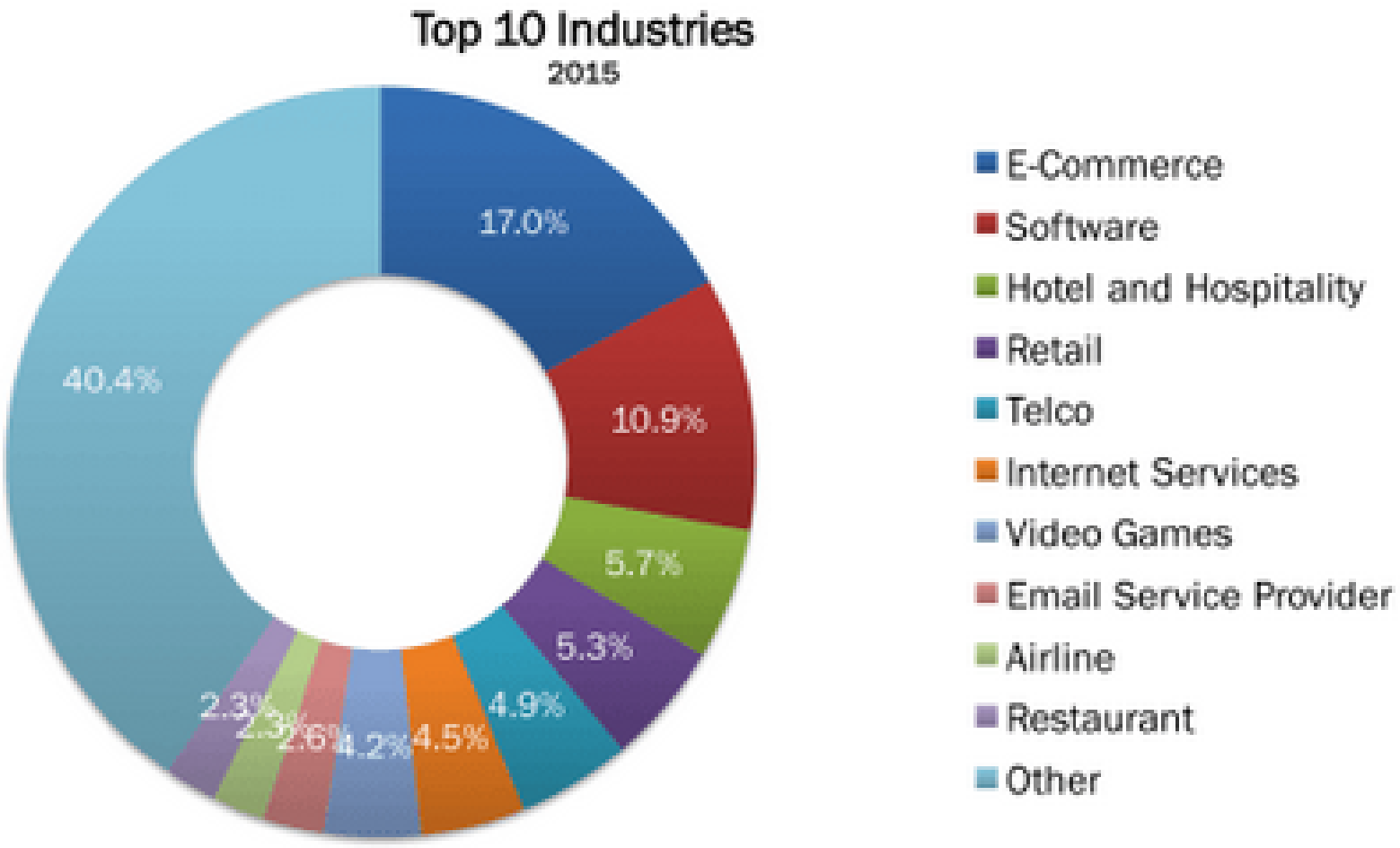


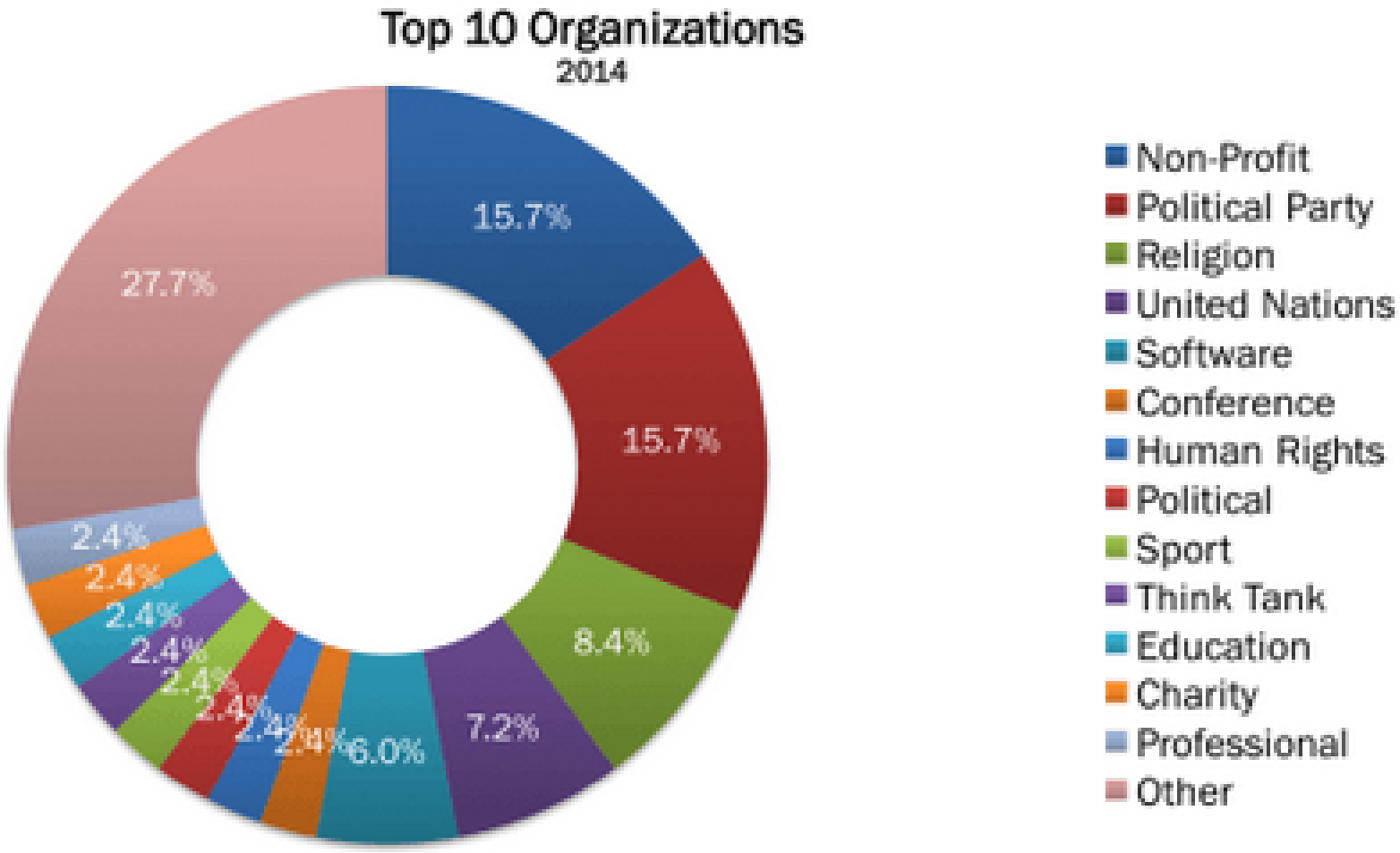
Source:Vontu risk assessment findings.

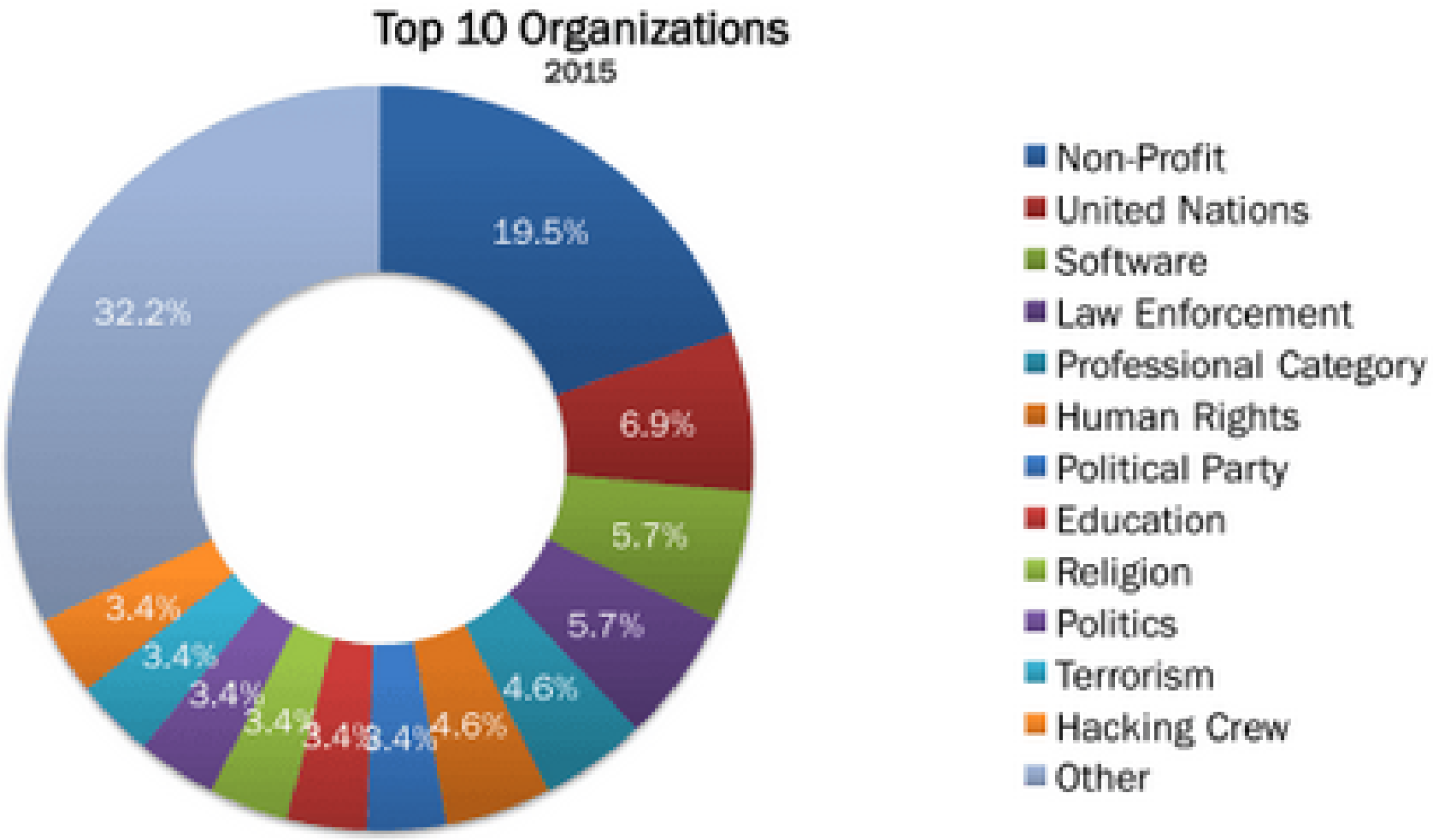

Top 10 Distribution of Targets
2014
33.8%
20.0%
9.4%
6.0%
5.7%
3.3%
3.1%
2.8%
2.5%
2.0%
11.4%
Industry
Government
Organization
Education
Single Individuals
>1
Healthcare
News
Finance
Online Services
Other

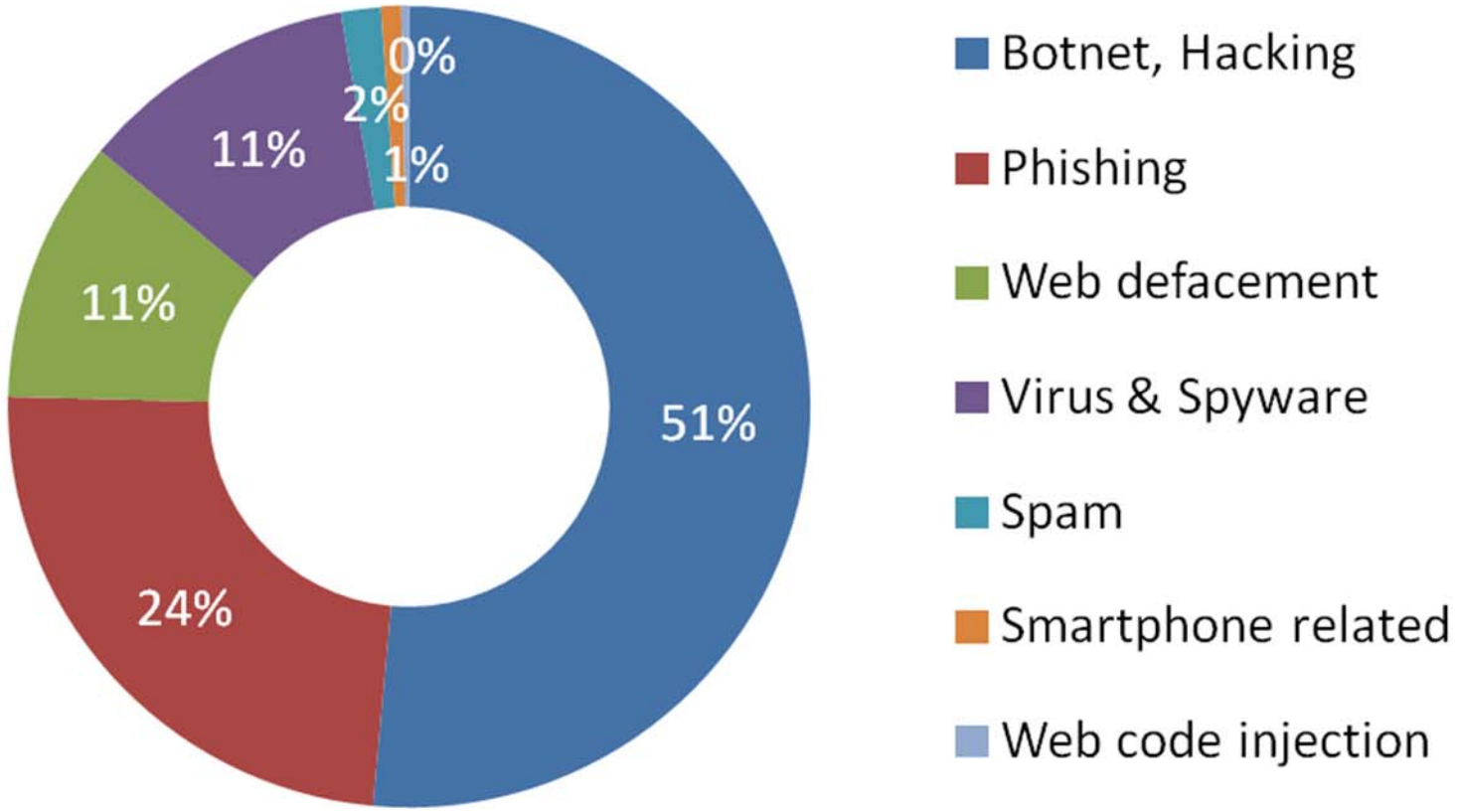

Top 10 Distribution of Targets
2015
25.2%
13.7%
8.3%
6.9%
4.9%
4.4%
2.9%
2.6%
2.6%
2.5%
26.2%
Industry
Government
Organization
Education
Single Individuals
>1
News
Finance
Healthcare
Online Services
Other

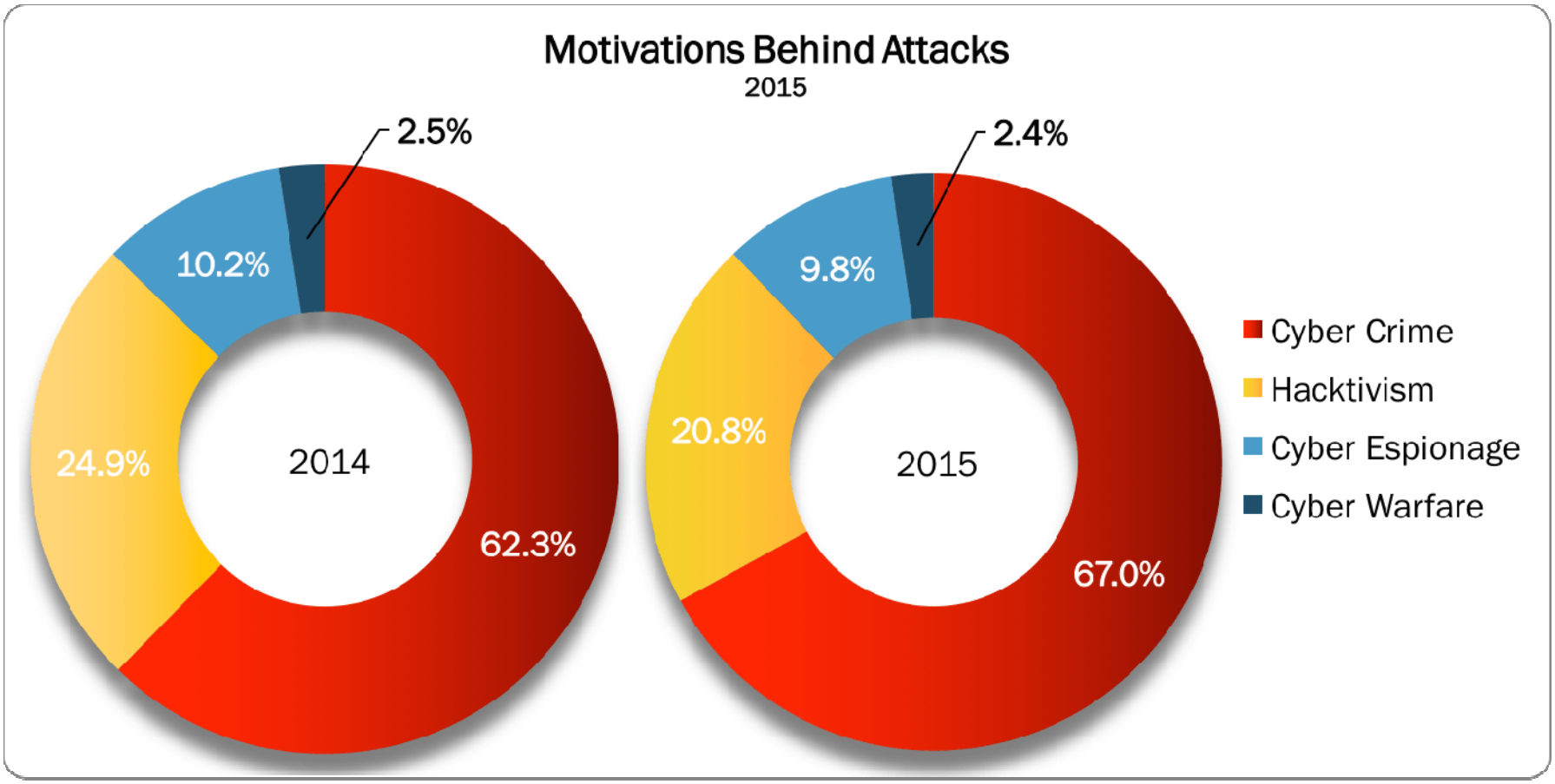

Top 10 Industries
2014
11.1%
10.1%
8.8%
6.4%
5.4%
4.7%
4.4%
4.0%
3.7%
1.7%
39.7%
E-Commerce
Software
Retail
Video Games
Hotel and Hospitality
Telco
Entertainment
Restaurant
Internet Services
Computer Hardware
Other

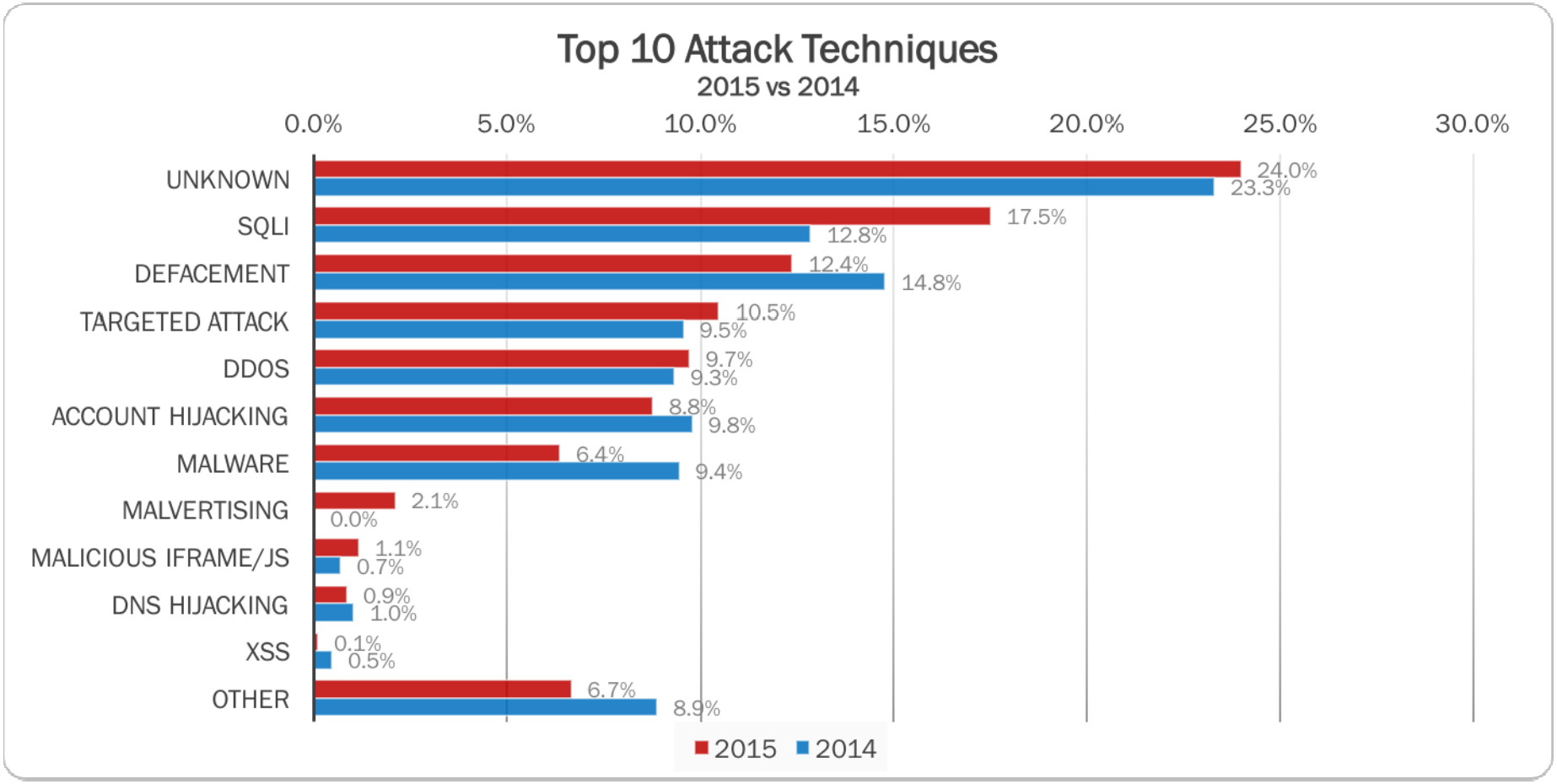

Top 10 Industries
2015
17.0%
10.9%
5.7%
5.3%
4.9%
4.5%
4.2%
2.6%
2.3%
2.3%
40.4%
E-Commerce
Software
Hotel and Hospitality
Retail
Telco
Internet Services
Video Games
Email Service Provider
Airline
Restaurant
Other

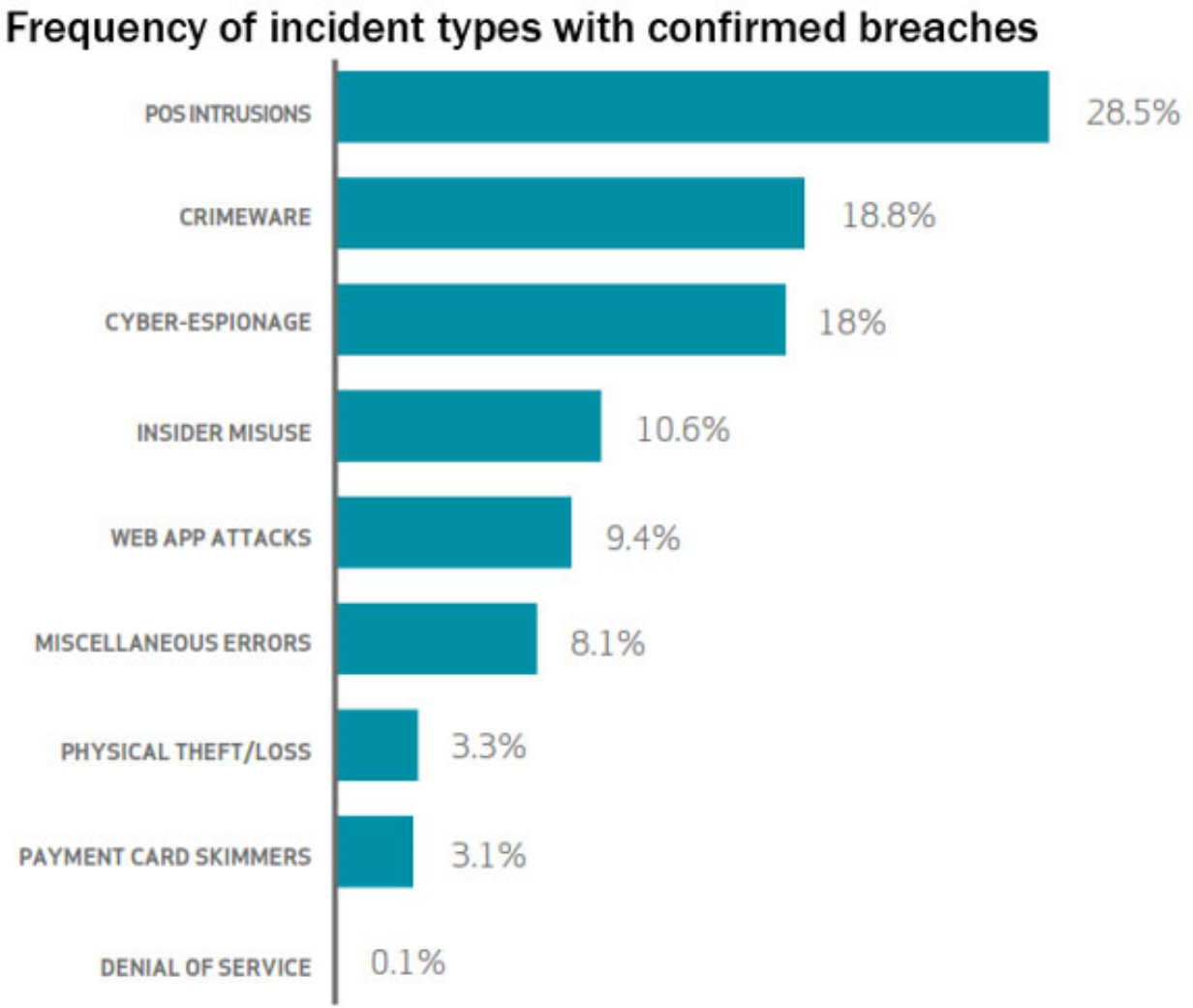

Top 10 Organizations
2014
15.7%
15.7%
8.4%
7.2%
6.0%
2.4%
2.4%
2.4%
2.4%
2.4%
2.4%
2.4%
2.4%
27.7%
Non-Profit
Political Party
Religion
United Nations
Software
Conference
Human Rights
Political
Sport
Think Tank
Education
Charity
Professional
Other


Top 10 Organizations
2015
19.5%
6.9%
5.7%
5.7%
4.6%
4.6%
3.4%
3.4%
3.4%
3.4%
3.4%
32.2%
Non-Profit
United Nations
Software
Law Enforcement
Professional Category
Human Rights
Political Party
Education
Religion
Politics
Terrorism
Hacking Crew
Other


0%
2%
11%
1%
11%
51%
24%
Botnet, Hacking
Phishing
Web defacement
Virus & Spyware
Spam
Smartphone related
Web code injection


Motivations Behind Attacks
2015
2.5%
10.2%
24.9%
62.3%
2014
2.4%
9.8%
20.8%
67.0%
2015
Cyber Crime
Hacktivism
Cyber Espionage
Cyber Warfare


Top 10 Attack Techniques
2015 vs 2014
0.0%
5.0%
10.0%
15.0%
20.0%
25.0%
30.0%
UNKNOWN
24.0%
23.3%
SQLI
17.5%
12.8%
DEFACEMENT
12.4%
14.8%
TARGETED ATTACK
10.5%
9.5%
DDOS
9.7%
9.3%
ACCOUNT HIJACKING
8.8%
9.8%
MALWARE
6.4%
9.4%
MALVERTISING
2.1%
0.0%
MALICIOUS IFRAME/JS
1.1%
0.7%
DNS HIJACKING
0.9%
1.0%
XSS
0.1%
0.5%
OTHER
6.7%
8.9%
2015
2014


Frequency of incident types with confirmed breaches
POS INTRUSIONS
28.5%
CRIMEWARE
18.8%
CYBER-ESPIONAGE
18%
INSIDER MISUSE
10.6%
WEB APP ATTACKS
9.4%
MISCELLANEOUS ERRORS
8.1%
PHYSICAL THEFT/LOSS
3.3%
PAYMENT CARD SKIMMERS
3.1%
DENIAL OF SERVICE
0.1%

Top Cyberattack and Data Breach Worries

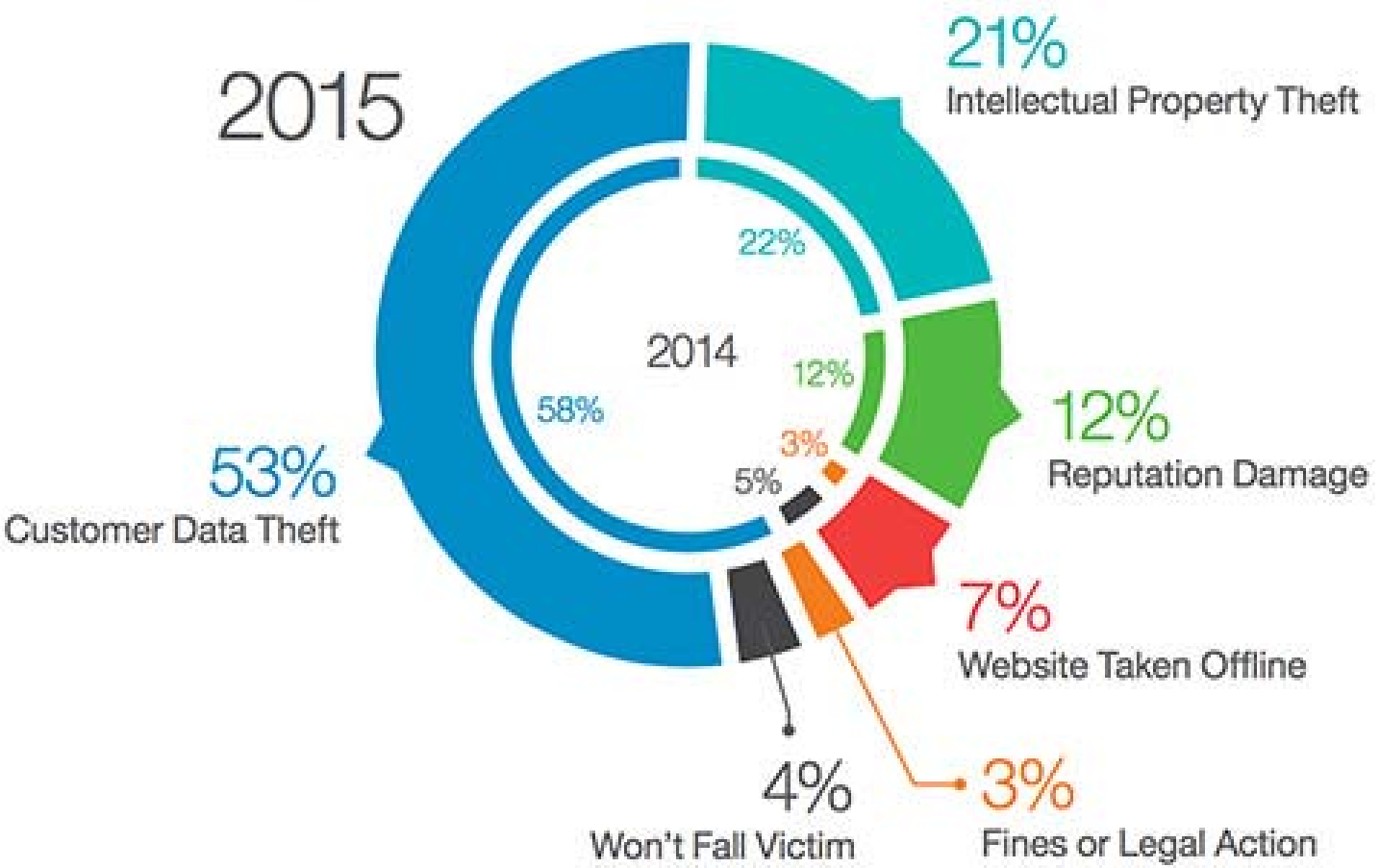
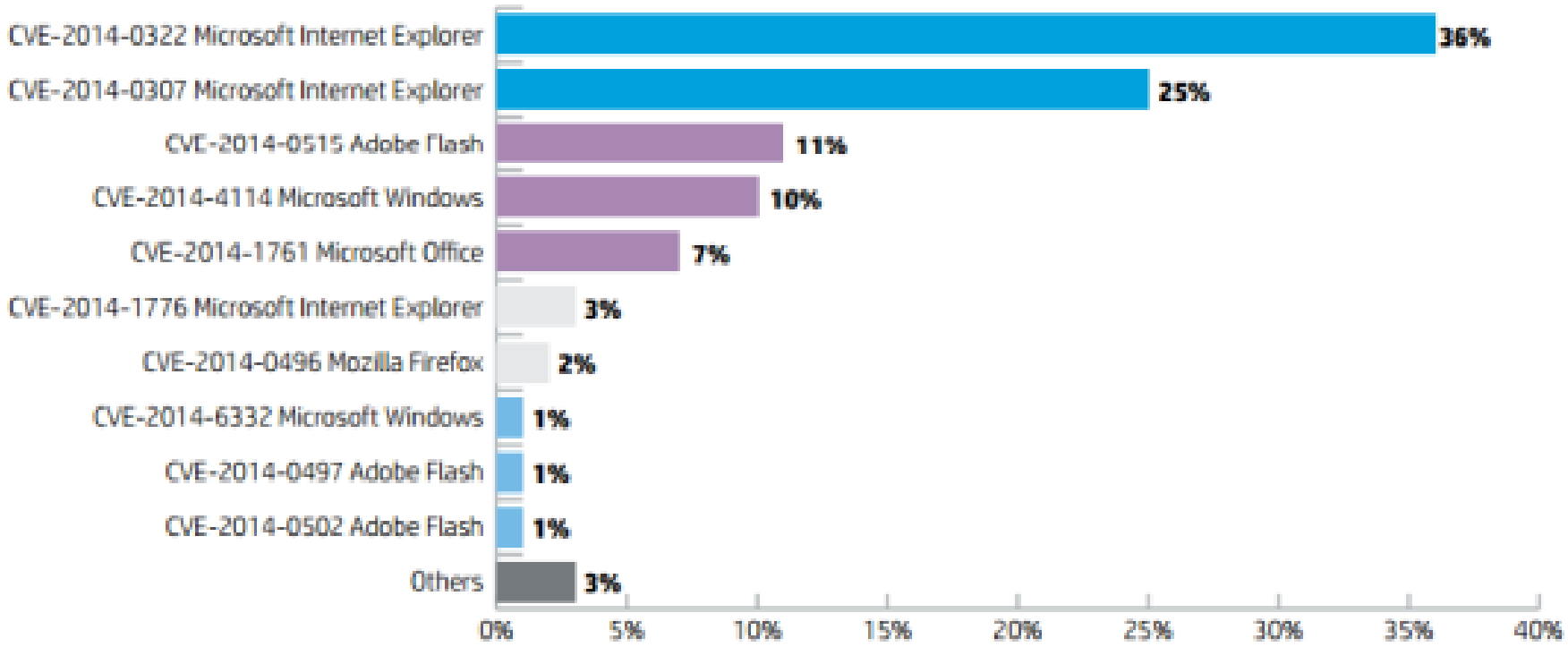
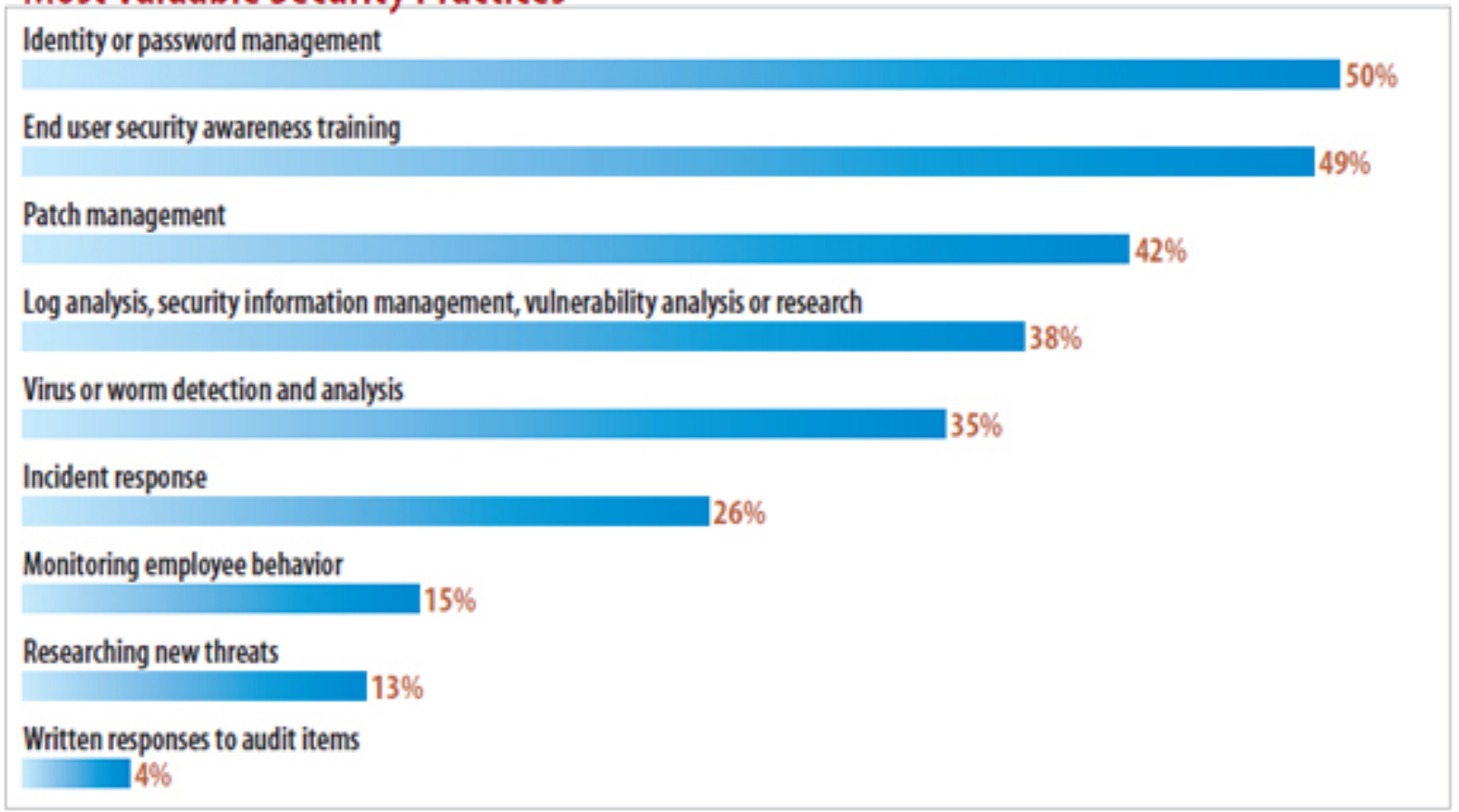


Figure 1. Top discovered CVE-2014 exploits



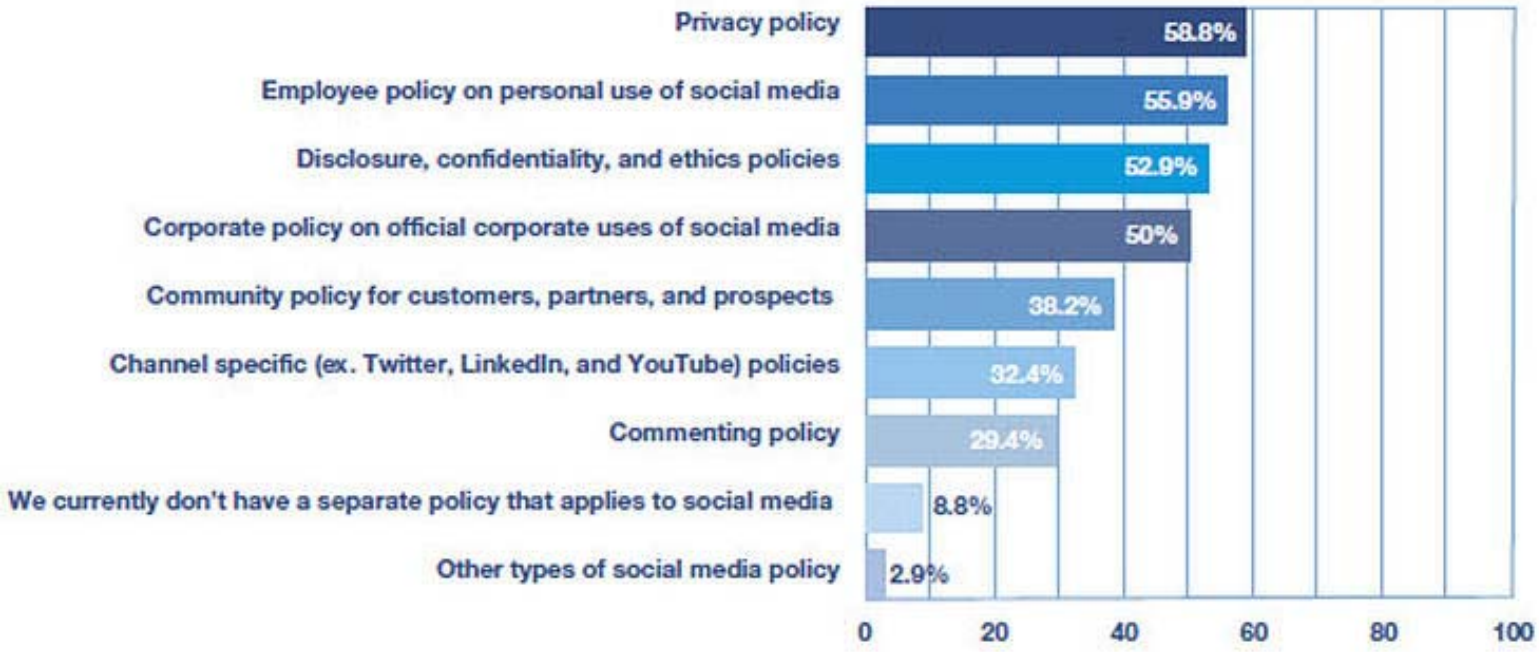
Most Valuable Security Practices



Data: *InformationWeek* 2012 Strategic Security Survey of 946 business technology and security professionals at companies with 100 or more employees, March 2012

Figure 9.1: Privacy Policy is the Most Common Social Media Policy

"Which of the following social media policies or other policies that either include social media or are referenced back to in social media policies does your company currently have?"

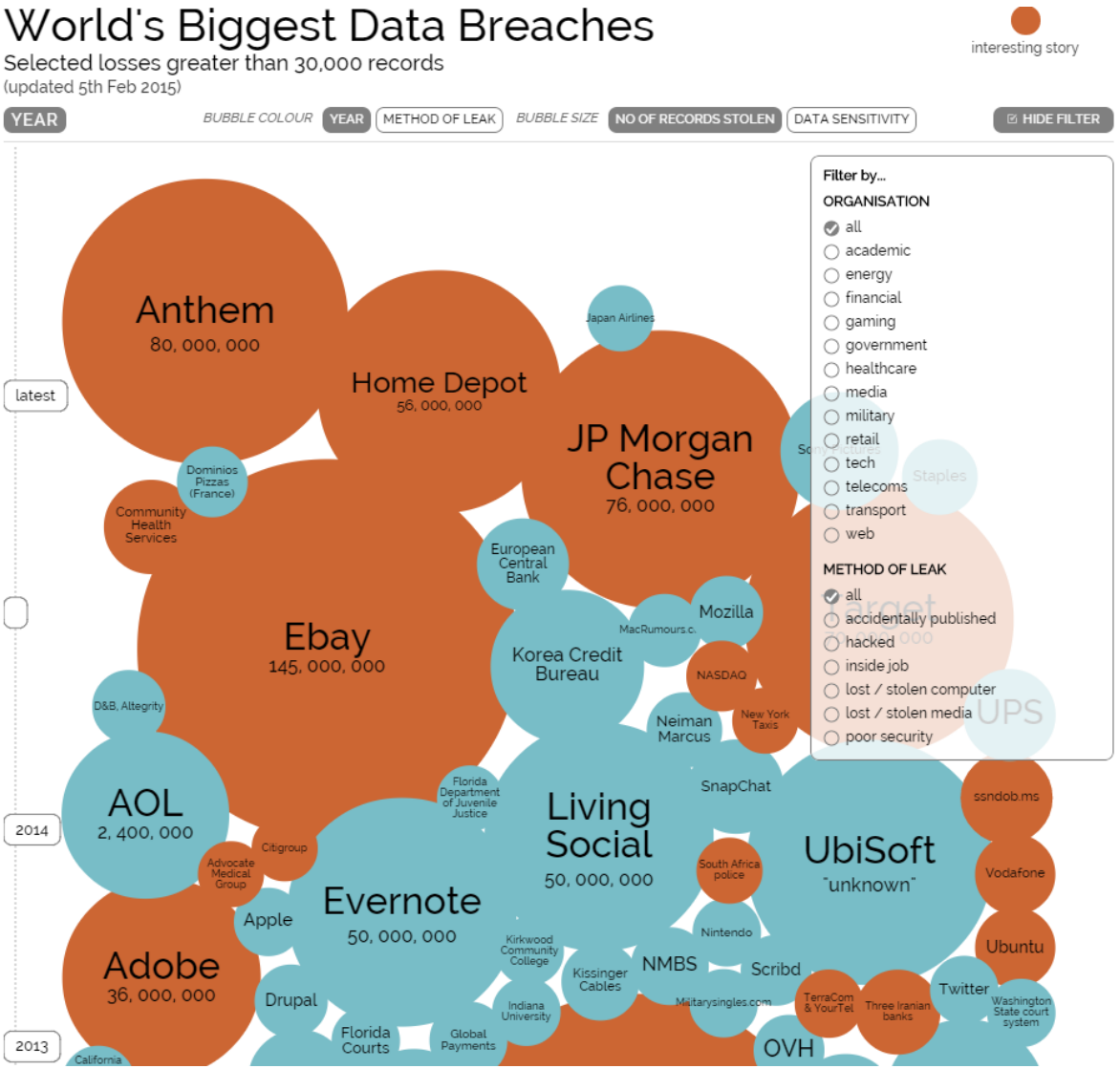


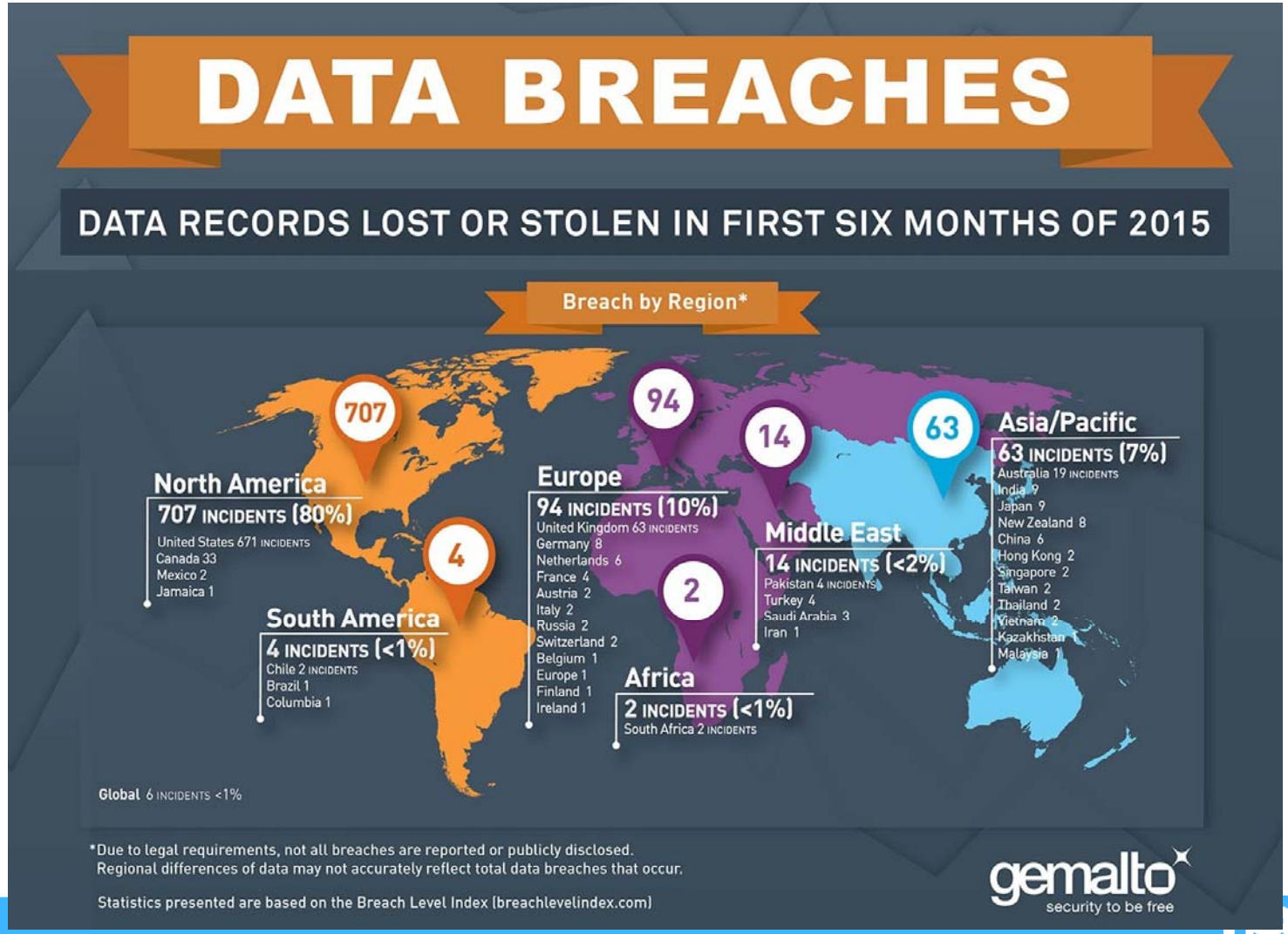
Base: 34 of 61 respondents for whom social media risk management is their primary or a significant part of their responsibility.

Source: "Guarding the Social Gates: The Imperative for Social Media Risk Management," Altimeter Group (Aug. 9, 2012)

ALTIMETER


DATA BREACHES
DATA RECORDS LOST OR STOLEN IN 2015
707,509,815
ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.
1,938,383
records lost or stolen
every day
80,766
records
every hour
24h
1,346
records
every minute
22
records
every second


World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 5th Feb 2015)
interesting story
YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
HIDE FILTER
Filter by...
ORGANISATION
all
academic
energy
financial
gaming
government
healthcare
media
military
retail
tech
telecoms
transport
web
METHOD OF LEAK
all
accidentally published
hacked
inside job
lost / stolen computer
lost / stolen media
poor security
latest
2014
2013
Anthem
80, 000, 000
Home Depot
56, 000, 000
JP Morgan Chase
76, 000, 000
Ebay
145, 000, 000
AOL
2, 400, 000
Adobe
36, 000, 000
Evernote
50, 000, 000
Living Social
50, 000, 000
UbiSoft
"unknown"
Japan Airlines
Dominios Pizzas (France)
Community Health Services
European Central Bank
Korea Credit Bureau
MacRumours.c.
Mozilla
NASDAQ
New York Taxis
Neiman Marcus
SnapChat
Staples
UPS
D&B, Altegrity
Florida Department of Juvenile Justice
Citigroup
Advocate Medical Group
Apple
Drupal
Florida Courts
Global Payments
Kirkwood Community College
Indiana University
Kissinger Cables
NMBS
Scribd
Militarysingles.com
South Africa police
Nintendo
TerraCom & YourTel
Three Iranian banks
Twitter
Washington State court system
Ubuntu
Vodafone
ssndob.ms
OVH
California


DATA BREACHES
DATA RECORDS LOST OR STOLEN IN FIRST SIX MONTHS OF 2015
Breach by Region*
707
North America
707 INCIDENTS (80%)
United States 671 INCIDENTS
Canada 33
Mexico 2
Jamaica 1
4
South America
4 INCIDENTS (<1%)
Chile 2 INCIDENTS
Brazil 1
Columbia 1
94
Europe
94 INCIDENTS (10%)
United Kingdom 63 INCIDENTS
Germany 8
Netherlands 6
France 4
Austria 2
Italy 2
Russia 2
Switzerland 2
Belgium 1
Europe 1
Finland 1
Ireland 1
2
Africa
2 INCIDENTS (<1%)
South Africa 2 INCIDENTS
14
Middle East
14 INCIDENTS (<2%)
Pakistan 4 INCIDENTS
Turkey 4
Saudi Arabia 3
Iran 1
63
Asia/Pacific
63 INCIDENTS (7%)
Australia 19 INCIDENTS
India 9
Japan 9
New Zealand 8
China 6
Hong Kong 2
Singapore 2
Taiwan 2
Thailand 2
Vietnam 2
Kazakhstan 1
Malaysia 1
Global 6 INCIDENTS <1%
*Due to legal requirements, not all breaches are reported or publicly disclosed.
Regional differences of data may not accurately reflect total data breaches that occur.
Statistics presented are based on the Breach Level Index (breachlevelindex.com)
gemalto
security to be free

چرا جلوگیری از نشت اطلاعات اهمیت زیادی دارد؟

- قبول وجود این مشکل
- محافظت از نام و شهرت سازمان
- هزینه بازسازی اطلاعات

زمان استراحت

با این موضوع فکر کنیم:

در سازمان من چه نقاطی دارای تهدید نشت اطلاعات هستند؟

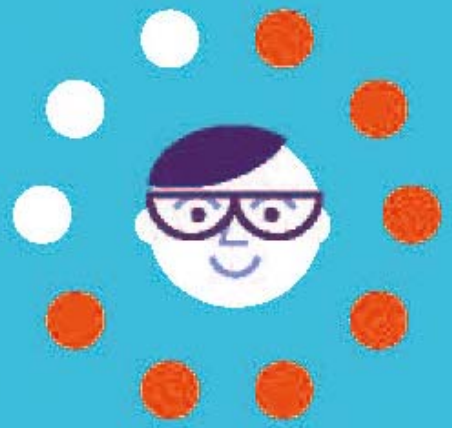
آیا وقوع رخدادهای امنیتی و نشت داده در داخل سازمانها و شرکت ها حقیقت دارد؟

قدم برای بررسی این موضوع

۱

بررسی کنید که کارکنان شما به چه اسناد و مدارکی دسترسی دارند.

اسناد مالی، پایگاه داده های مشتری، استراتژی بازاریابی



آیا میدانید ۷ نفر از ۱۰ پرسنل
به فایل های محرمانه دسترسی دارند
و از آنها در کار روزانه خود استفاده میکنند ؟

آیا میدانید ۶ نفر از ۱۰ پرسنل
آگاه نیستند که کدام فایل محرمانه هست و کدامیک محرمانه نیست ؟

آیا میدانید ۴ نفر از ۱۰ پرسنل
می تواند برای شما یک ماجرا از ارسال اطلاعات محرمانه در رسانه های اجتماعی
و یا جاهای دیگر توسط همکارانش تعریف کند ؟

۲

بررسی کنید کارمندان شما
از چه ابزارهایی برای به اشتراک گذاری فایلها استفاده می‌کنند؟

Skype, Dropbox, Outlook, USB devices

90%

٪۹۰ کارمندان از Outlook برای به اشتراک گذاری فایل با همکاران و سایرین استفاده میکنند .

۴۶٪ از همکاران فایل های کاری را بر روی کامپیوترهای شخصی خود کپی می کنند
یا از خارج از محل شرکت به شبکه شرکت وصل میشوند تا کارهای خود را در خانه انجام دهند .

TOP 3

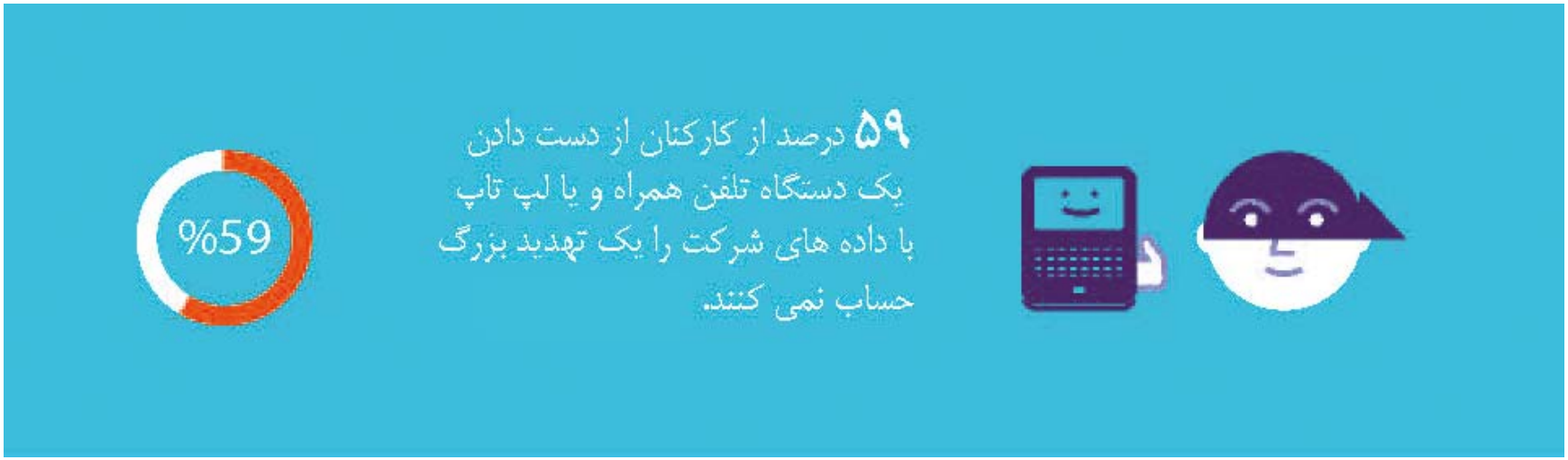
آیا میدانید یکی از **۳ عامل بزرگ نشت اطلاعات**
در سراسر جهان استفاده از USB رمز گذاری نشده است ؟

2 1 3

ایجاد یک آزمون کوتاه برای سنجیدن
میزان دانش کارکنان پیرامون امنیت داده ها


%18
* * * * * * *
۱۸ درصد از کارکنان
رمزهای خود را با همکارانشان به اشتراک میگذارند .


%35
۳۵ در صد از کارکنان
امنیت اطلاعات را مسئولیت خود نمیدانند .


۵۹ درصد از کارکنان از دست دادن
یک دستگاه تلفن همراه و یا لپ تاپ
با داده های شرکت را یک تهدید بزرگ
حساب نمی کنند.
%59

۴ مشخص کنید آیا سیستم امنیتی فعلی شما می تواند نفوذ نیروهای خودی را در صورت اتفاق تشخیص دهد .

%50

۵۰ درصد از کارکنان
ایمیل به شخص اشتباه فرستاده اند .

آیا می توانید مشخص کنید چه
کسی گزارشات مالی را به یک
گیرنده مشکوک ارسال کرده است؟

۶۳ درصد از شرکتها نمی توانند راه حلی مطمئن برای جلوگیری از از دست دادن داده ها قبل از اتفاق پیدا کنند .

چه اتفاقی می افتد اگر کاربران اطلاعات محرمانه را کپی وبه Google Drive ارسال کنند ؟

۶۸ درصد از کارکنان ترجیح می دهند ایمیلهای شرکتی خود را برای استفاده در مواقع اضطراری ، روی گوشی های هوشمند خود هم داشته باشند .

%68

آیا می دانید چه تعدادی از کارکنان شما ایمیل های شرکتی خود را همزمان بر روی گوشی های هوشمند خود دریافت میکنند ؟

آیا تحقیقات شما میتواند خسارتها و زیانهای مالی ناشی از نشت اطلاعات را مشخص کند ؟

آیا شرکت شما میتواند این هزینه ها را جبران کند ؟

۴۰٪ از مشتریان بالقوه نمی خواهند با شرکتهایی که
دچار نشت اطلاعات هستند کار کنند.

4.8$

۴/۸ میلیون دلار بالاترین مبلغی است که تا سال ۲۰۱۴ برای حل و فصل معضلات ناشی از نشت اطلاعات پرداخت شده است.

3.5$

۳/۵ میلیون دلار متوسط هزینه خسارت داده های اطلاعاتی است.

نشت اطلاعات از چه درگاههایی اتفاق می افتد؟

نشت اطلاعات

مشخصه های بررسی وضعیت:

اطلاعات محرمانه من کجا ذخیره می گردد؟

Data at Rest

اطلاعات محرمانه قابل حمل من چگونه مورد استفاده قرار می گیرد؟

Data in Motion

نشت اطلاعات در کجاها رخ می دهد ؟

Data Policy Enforcement/Data at Endpoint

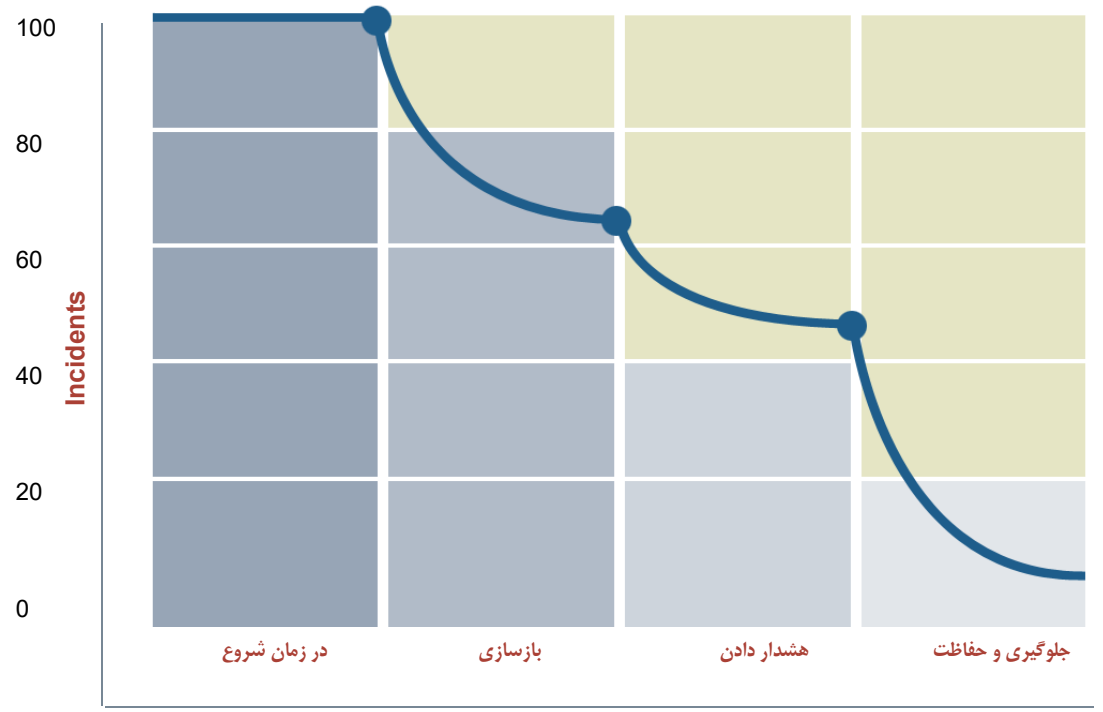
الزام به اجرای سیاست ها برای کاهش مخاطرات

سطوح الزام

1. بازسازی
2. هشدار دادن
3. جلوگیر و محافظت

چگونه ریسک کاهش می یابد؟

- ترمیم پردازش های قطع شده
- آموزش پرسنل
- هشدار به نقض کنندگان قوانین
- اطلاع رسانی به مدیر
- محافظت از فایل ها
- جلوگیری از حوادث



روش شناسایی و محافظت از داده های ذخیره شده

تعریف سیاست های داده های محرمانه

1

اجرا، پویش و پیداکردن داده های در معرض خطر

2

اعمال سیاست ها بصورت خودکار برای فایل های مورد نظر

3

بازبینی مخاطرات

4

گزارش از لیست های قابل پذیرش

5

کنترل و جلوگیری از نشت اطلاعات محرمانه در داده های در حال انتقال

شناسایی پرسنلی که باید اطلاعات محرمانه ارسال نمایند.

1

تشخیص یا جلوگیری از وقوع حادثه

2

هشدار به پرسنل

3

بازنگری گردش کارهای اتوماتیک

4

گزارش از مخاطرات و مخاطرات پذیرفته شده

5

راه حل ارسال پیام امن

شناسایی پرسنلی که اطلاعات محرمانه ارسال می کنند.

1

شناسایی مخاطرات

2

نشانه گذاری ایمیل ها

3

استفاده از ابزاری که صورت خودکار ایمیل های نشانه گذاری شده را کد نماید

4

گزارش از مخاطرات و مخاطرات پذیرفته شده

5

الزامات جلوگیری از نشت اطلاعات

- تشخیص و محافظت داده های محرمانه
- نظارت و جلوگیری ازنشت داده های در حال جابجایی
- تشخیص دقیق در تمامی گروه ها و محتواها
- مکانیزم اجرا و پاسخگویی خودکار در گردش کارها
- کدسازی داده های مشهود و کنترلی
- حفاظت از حریم خصوصی کارمندان
- تایید حجم داده های مهم و معماری مورد نظربرای پیاده سازی سیستم

ارزیابی ریسک ها

- چه تعداد ایمیل از شرکت شما خارج می شود؟
- چه کسانی اطلاعات محرمانه را ارسال می کند؟
- چه پروتکولهایی بیشترین حملات را داشته اند؟
- چه تعدادی از این ایمیل ها نقض کننده قوانین هستند؟
- سطح ریسک سازمان شما در مقابل شرکت ها و رقبای همتراز شما چه اندازه است؟

RISK ASSESSMENT SCORECARD

الویت داده	احتمال از دست	Data At Rest		Data in Motion	
		Frequency	Risk	Frequency	Risk
اطلاعات سازمان	High	High 721 incidents	 Very High	High 256 incidents	 Very High
اطلاعات مشتریان	High	High 10,178 incidents	 Very High	High 2178 incidents	 Very High
نظرات کارشناسان شرکت	High	Very High 78 incidents	 Very High	Medium 9 incidents	 Medium
اطلاعات مدیریتی	High	Medium 939 incidents	 High	Medium 132 incidents	 High
تحقیقات	High	High 624 incidents	 High	High 24 incidents	 High

ریسک = میزان وقوع x احتمال وقوع

جمع بندی

- کاهش ریسک از دست دادن اطلاعات
- کاهش ضررهای مالی
- حفاظت از نام سازمان و تداوم کسب و کار
- بررسی تطابق های استانداردی

> Security is not a product, but a process.
>
> Bruce Schneier

با سپاس