# BE CAREFUL OUT THERE

It's a compliance and security minefield.

The game has changed for the customer experience industry, and providing superior service isn't enough. Cyber-attacks, regulatory oversight, fraud and constant legal threats require a dedicated compliance focus to protect your brand and your customers.

#### CYBER ATTACKS. HACKING. FRAUD.

How big is the threat?



In 2014, Cybercrime costs the global economy up to \$575 billion annually. The U.S. took a \$100 billion hit, the largest of any country.1



40 MILLION people in the U.S.

& 80 MILLION individuals worldwide had personal records stolen in 2013.1



Consumers fear having their identity stolen more than any other crime they were asked about. An overwhelming **69%** of consumers share this fear.<sup>2</sup>



\$16 Billion Stolen from 12.7 Million Identity Fraud Victims in 2014.

of Identity Fraud Victims were also



Last year, the FBI notified 3,000 US companies—ranging from small banks, major defense contractors, and leading retailers—that they had been victims of cyber intrusion.4

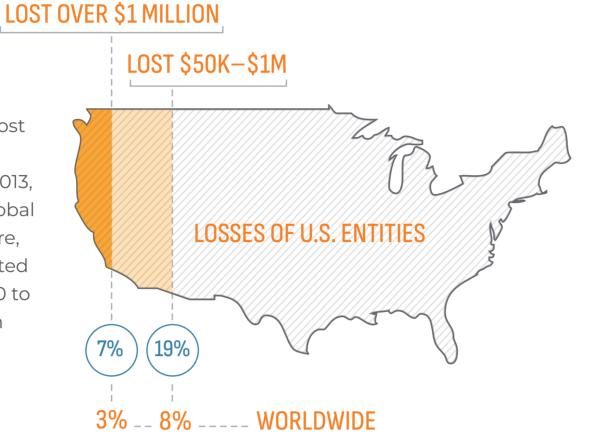


Notified Data Breach Victims.<sup>3</sup>



7% of US organizations lost \$1 million or more to cybercrime incidents in 2013, compared with 3% of global organizations; furthermore, 19% of US entities reported financial losses of \$50,000 to \$1 million, compared with 8% of worldwide

respondents.4





incident were not able to estimate the financial costs. Among those that could,

estimate the costs, the average annual monetary loss was approximately \$415,000.

### WHAT'S ON THE HORIZON? What do you need to plan for?





Relentless threats of cyber campaigns, cyberwarfare, cyberterrorism





threats

External government





5

Internal corporate compromise intended to defraud



6

Rapidly evolving and stringent regulatory and compliance requirements



Increased management of company reputational





Data security in a world of data proliferation

## HOW DO I PROTECT MY BRAND AND MY CUSTOMERS?

Embrace a corporation-wide data security culture. This should include:

Data security policy, procedure and training, including: Security Awareness Training, Penetration Testing, Payment Card Industry (PCI) data security standards if applicable to your business.

#### Establish a Compliance Management System (CMS) to include:



#### OFFER SAFETY TIPS FOR YOUR CUSTOMERS, OFFERED BY JAVELIN RESEARCH6: • Secure mobile devices. • After a data breach, make sure that any

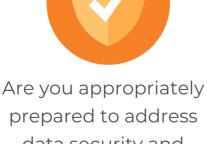
- Exercise good password habits.
- Take advantage of EMV chip cards and mobile payments.
- Sign up for account alerts.
- Seek help as soon as fraud is detected. Notify financial institutions, credit card issuers,

"free monitoring services" fit the crime.

wireless carriers or other service providers. Also, contact credit report agencies.

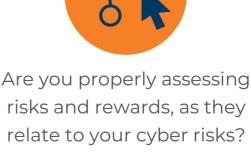
### IN MIND?

WHAT ELSE SHOULD I KEEP



data security and compliance risks? Are you keeping up with technology?





### FIND OUT MORE AT alorica.com

1. McAfee 2014 Report - Net Losses: Estimating the Global Cost of Crime, June 2014.

REFERENCES

- 2. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?ncid=txtlnkusaolp00000618
- 3. http://www.reuters.com/article/2015/03/03/ca-javelin-strategy-idUSnBw035247a+100+BSW20150303 4. http://www.pwc/cybersecurity, June 2014
- 5. http://dev.webrecon.com/debt-collection-litigation-cfpb-complaint-statistics-december-2014-and-year-in-review/ 6. http://javelin.com