Security Risks Equal Business Risks

It should come as no surprise that the number of cyber-attacks continues to rise. As noted in Radware's *2015-2016 Global Application & Network Security Report*, more than 90% of respondents reported experiencing attacks in 2015.

But what are the costs of actually "cleaning" up after a cyber-attack? What are the potential impacts of these assaults on business, and do partners who interact or share networks with a business pose a security threat? To find out, Radware conducted a survey of more than 200 C-level security executives from the U.S. and United Kingdom.

In the *Security and the C-Suite: Threats and Opportunities Report*, executives underscored just how expensive recovering from a cyber-attack is. More than a third of respondents in the U.S. said an attack had cost them more than $1 million, and 5% said they spent more than $10 million. Costs in the U.K. were generally lower, with 63% saying an attack had cost less than £351,245 (or about $500,000), though 6% claimed costs above £7 million.

Estimated Cost of an Attack

	COUNTRY	
	U.S.	**U.K.**
Less than $100,000/Less than £70,249	15%	12%
$100,001-$250,000/£70,250-£175,622	14%	34%
$250,001-$500,000/£175,623-£351,245	18%	17%
$500,001 but less than $1M/£351,246-£702, 490	16%	10%
$1M but less than $3M/£702,500-£2.1 million	14%	12%
$3M but less than $5M/£2.1 million but less than £3.5 million	9%	9%
$5M but less than $10M/£3.5 million but less than £7 million	8%	1%
$10M+/£7 million or more	5%	6%

Figure 1: Estimated Cost of an Attack

Given the prevalence and cost of security incidents, it is not surprising that four out of five executives (82%) say that security threats are now a CEO or board-level concern. That's a notable increase from a 2014 executive survey conducted by Radware, which found that security was a CEO or board-level concern for less than three-quarters of respondents.

The 2016 Executive Report affirmed that partners remain an area of potential weakness. Every partner that interacts with a business or its network should adhere to the same security standards. To their credit, 44% of respondents have been including suppliers and partners in security processes for more than two years and another 33% have begun doing so within the past two years. However, more than one-fifth (22%) are still not addressing suppliers and partners in their processes. When asked what partners and customers are asking related to enhanced security, about two-fifths of executives said "none" or gave no specific answer.

Security Threats are a Board Level Concern

The majority of respondents indicate that security threats are now a CEO or board-level concern in their company.*

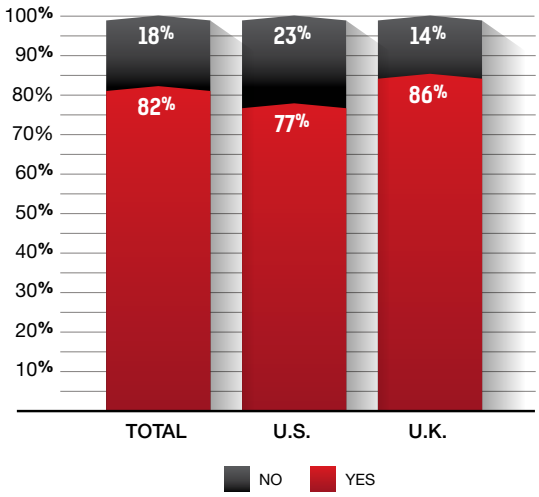

Figure 2: Security Threats Are a Board-Level Concern

* This is slightly higher for those in the U.K., compared to those in the U.S.

The 2016 Executive Report also confirmed the potential impact of security threats. Executives rated brand reputation, operational loss and revenue loss as the areas of greatest impact. Among the other potential effects cited: productivity loss, impact on share price value, unexpected increases in budget, training/education and hiring requirements, and contract loss. The impacts selected were largely the same among U.S. and U.K. executives, with one exception: business leaders in the U.K. were more likely to mention unexpected contract loss as a top concern.

Impact of Security Threats on Business

		COUNTRY	
RANKED 1st/2nd	**TOTAL**	**U.S.**	**U.K.**
Brand Reputation Loss	34%	38%	31%
Operational Loss	31%	31%	32%
Revenue Loss	30%	34%	27%
Productivity Loss	24%	27%	21%
Share Price Value	18%	16%	20%
Unexpected Budget Increases	17%	14%	19%
Unexpected Training/Education	16%	16%	16%
Unexpected Hiring Requirements	15%	14%	16%
Unexpected Contract Loss	15%	10%	20%

- Security threats are most likely to cause the biggest losses to a company's brand reputation, operations, and revenue.
  - These areas are rated as first or second in terms of greatest impact by executives.
- Executives in the U.S. and U.K. rate the impacts similarly with the exception of unexpected contract loss which is more likely to be rated as a greatest or second greatest impact compared to those saying the same in the U.S.

Figure 3: Impact of Security Threats on Business

Above all, the report confirmed that companies continue to take action—but still have opportunities to do more. In both the U.S. and the U.K., about one-third of executives rate changes in technology, C-level awareness or knowledge/education as critical to effectively thwarting security threats. Process and policy changes are extremely important to almost three in 10 executives, with just one in five pointing to changes in resources as critical to dealing with security threats.

Importance of Changes to Thwart Security Threats

EXTREMELY IMPORTANT (CRITICAL)	TOTAL	COUNTRY	
		U.S.	U.K.
Changes in Technology	35%	36%	34%
Changes in C-Level Awareness	33%	34%	32%
Changes in Knowledge/ Education	32%	31%	34%
Changes in Process	28%	31%	26%
Changes in Policy/ Procedure	28%	32%	24%
Changes in Resources	22%	19%	24%

- About one-third of the executives rate changes in technology, C-level awareness, or knowledge/education as extremely important/critical in effectively thwarting security threats.
- Process and policy changes are extremely important to 30% of executives, and one in five say changes in resources are critical in dealing with security threats.
- Importance is consistent between the U.S. and the U.K.

Figure 4: Importance of Changes to Thwart Security Threats

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.