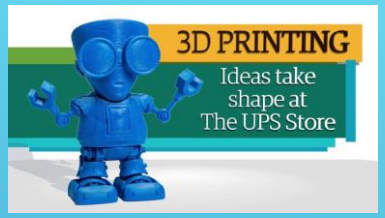
THE BUSINESS OF SECURITY

Sandy Carielli
Security Technologies Director
Entrust Datacard
sandy.carielli@entrustdatacard.com
@sandycarielli

SECURITY AND BUSINESS



By 2020, 75% of businesses will be digital

THE RISE OF DIGITAL BUSINESS

DIGITAL BUSINESS, SECURITY AND RISK

Rather than eliminate risk, accept and implement controls to help enable business

HOW

SECURITY AS A BUSINESS ENABLER: A CONTROL THAT MAKES YOU FASTER

PRIORITIZATION

WHAT "MUST" BE DONE

YOUR BUDGET

Bulletin (SB16-291)

More Bulletins

Vulnerability Summary for the Week of October 10, 2016

Original release date: October 17, 2016

Print Tweet Send Share

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

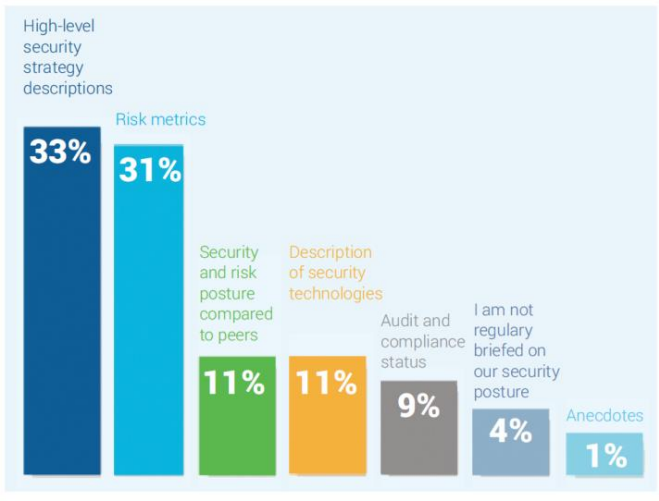
COMMUNICATION

A STORY ABOUT SECURITY RISK AND POOR COMMUNICATION…

CISO Qualities
What do you see as the key qualities of a chief information security officer (CISO)?

1. Technical skills and experience
2. Business acumen
3. Strong communicator
4. Risk taker
5. Crisis communication expert

IT Security
How do you prefer information regarding cybersecurity be presented?



STRATEGIC RATHER THAN TECHNOLOGIST

Source: Veracode/NYSE

1. Stage your meetings
2. No jargon
3. Stay focused
4. Talk risk – but think about acceptable risk
5. Talk cost of exposure and recovery – and measure against value

SPEAKING THEIR LANGUAGE: SANDY'S (UPDATED) RULES FOR SECURITY LEADERS

TALKING TO THE BUSINESS

SCENARIO #1

- It's a month until the big release of your company's product is about to ship. Many customers are waiting for this release, and it's likely to make the company $20M in additional revenue in the first month alone. You have found a security bug that you believe is high severity. A fix could delay the release by several weeks.
  - How do you assess the risk and impact?
  - How do you communicate that to the business?

SCENARIO #2

- You would like to hire an outside consulting firm to do some "ethical hacking" of your products and identify vulnerabilities. This will cost approximately $250,000 per year. You do not have this money in your budget, and you'd like to ask for it.
  - How do you justify the cost?
  - How do you explain the benefits of such a service?

- This morning, an unknown attacker staged a Distributed Denial of Service (DDoS) attack against your website, bringing it down for a couple of hours. Customers are concerned and the attack has been reported about in the media. You need to report to the board:
  - What happened?
  - How did this happen?
  - How did we get back online?
  - What do we need to do in the near term and longer term to reduce the risk of this happening again?
  - What should we tell the media and our customers?

SCENARIO #3

QUESTIONS?

THANK YOU!

Sandy Carielli

Security Technologies Director, Entrust Datacard

sandy.carielli@entrustdatacard.com

@sandycarielli