Agenda

• Intros
• Blue Lava InfoSec Survey Research and Findings
• Evolution – How Did We Get Here?
• What Organizations Are Doing
• Some Final Thoughts
About Me

• First computer at 12 then recruited by the military at 16
• Inventor of several InfoSec and Data Protection patents
• Implemented Information Security and Fraud solutions
  – DOD
  – Cheaptickets / eBookers / Galileo International / Orbitz
  – EDS/HP
  – Calyon Financial / NewEdge Financial / Societe General Group
  – Sears Online
• Multiple graduate degrees and security certifications
• Two-time former CISO, PCI QSA
• Gartner refers to work in the area of Big Data for Information Security and Fraud analytics
Sears Online Interview
The Perfect Grill ... for a Cannibal

Sure, Christmas is still 4 months away -- but if you have any friends who love to dine on human flesh, we've found the perfect gift for you ... courtesy of Sears?!

The department store is currently offering a grill on their website under the categories, "Human Cooking > Grills to Cook Babies and More > Body Part Roaster."
Altered Sears Web Site Offers Grill to 'Cook Babies'

By Joshua Rhett Miller / Published August 20, 2009 / FoxNews.com

The Web site for department store giant Sears offered a gruesome sales pitch Thursday — a grill that could "cook babies" and be used to roast body parts.

The goof, first reported by TMZ.com, listed any grill viewed by visitors to the company's Web site under the category of "human cooking > Grills to Cook Babies and More > Body Part Roaster."

The wording apparently was the work of a mischievous customer and, when discovered, was quickly changed, but not before TMZ.com captured a screenshot.

Representatives from Sears said they were victimized by "someone visiting" the company's Web site.

"We discovered earlier today that someone visiting our site had defaced a limited number of product pages," the company said in a written statement to FOXNews.com. "We've already taken steps to prevent this from happening again."

The company apologized for the incident and said there was no reason to believe customer data was intercepted during the security lapse.
InfoSec Research and Strategy
Approach and Quantitative Methodology for 2015 Data Collection

• Anonymous Survey
  – 15 InfoSec questions
  – Email distribution to targeted list
• > 300 participants
• Audience
  – Board of Directors and Executive Leadership Teams
  – InfoSec/Fraud Industry Practitioners and Engineers
What’s Top of Mind?

• Current architecture in most firms is a “hot mess”
• The perimeter is gone
• Internet of Things (IoT) is here
• Cybercriminals are bypassing traditional security systems easily
• InfoSec alignment with the Business is increasing
Some of the Blue Lava Survey Results
Is there Board Oversight with your InfoSec program?
Is cyber risk part of your current risk management framework?
Do you share incident information with industry groups?

Yes

No

Don't Know
How are you recruiting qualified and trained InfoSec professionals?

- Industry trade shows or professional organizations
- Through universities and colleges
- Traditional website recruitment
- Word of mouth
- Working with external recruiters
- Working with internal recruiters
- Working with staff aug or temp agencies
- Other (please specify)
My budget over the past year has....

![Graph showing budget changes]

- **Increased**
- **Decreased**
- **Same**
My breach predictions for 2015 are that InfoSec breaches will....
Which emerging technologies does your organization work with today?

Cloud: 90.0%
DevOps: 50.0%
Internet of Things (IoT): 40.0%
Mobile: 70.0%
OpenStack: 30.0%
Virtualization: 80.0%
Wearables: 10.0%
All of the above: 10.0%
Other (please specify): 10.0%
Evolution of Technology and Products

- Product
- Smarter Product
- Smarter Connected Product
- Product Integrated System
Evolution of the Automobile
Evolution of the Automobile

1 Product

2 Smarter Product
Evolution of the Automobile

1 Product

2 Smarter Product

3 Smarter Connected Product
Evolution of the Automobile

1. Product
2. Smarter Product
3. Smarter Connected Product
4. Automobile Intergrated System
System of Systems
Evolution of the Home
Evolution of the Home

1 Product

2 Smarter Product
Evolution of the Home

1. Product
2. Smarter Product
3. Smarter Connected Product
Evolution of the Home

1 Product

2 Smarter Product

3 Smarter Connected Product

4 Product System
Interconnected System of Systems
Interconnected System of Systems
How Did We Get Here?

Third Party Vendor

Traffic

N

Web

FIREWALL POLICY

Apps

FIREWALL POLICY

DBs

FIREWALL POLICY
Evolution – The Agile Data Center

Limited Visibility

- Third Parties
- Cloud

No Visibility to Internal Traffic
Evolution – The Agile Data Center

Limited Visibility

- Third Parties
- Cloud

No Visibility to Internal Traffic

No Visibility to Internal Traffic
Evolution – The Agile Data Center

Limited Visibility
- Third Parties
- Cloud

No Visibility to Internal Traffic

No Visibility to Internal Traffic

VM

VM

VM

VM

VM

VM

VM

VM

VM

VM

VM

VM

VM
Evolution – The Agile Data Center

Limited Visibility
- Third Parties
- Cloud

No Visibility to Internal Traffic

No Visibility to Internal Traffic
Where Do We Go From Here?

• Information Security must be part of the culture – driven by the Board of Directors and Executives throughout the organization

• Cyber criminals are evolving – we must as well

• Architecture and technical designs must be conducted earlier

• Include InfoSec exit criteria through all project deliverables

• It’s not if the cyber criminal will access your environment – it’s when – invest in current technologies and have a plan to address the issue - user behavior analytics (UBA) is critical

• Evaluate your InfoSec and IT Audit programs frequently – ensure part of the program is to evaluate emerging technology
Resources

• How to Measure Anything, Douglas W. Hubbard

• Hoernecke, Andy, Application Security, Data Visualization Expert, and Inventor of D3Dash
  www.d3dash.com

• Iron-Clad Java: Building Secure Web Applications, Jim Manico and August Detlefsen

• Litan, Avivah, VP and Distinguished Analyst, Gartner
  Market Guide for User Behavior Analytics (UBA), G00260457, August 2014

• Measuring and Managing Information Risk: A FAIR Approach, by Jack Freund and Jack Jones

• Perceptual Edge
  www.perceptualedge.com

• Security Metrics: Replacing Fear, Uncertainty, and Doubt, Andrew Jaquith

• threatTRANSFORM, Open Source Tool for creating and managing STIX data sets
  www.threattransform.com
Blue Lava
InfoSec Update

Thank You!

Laz

laz@blue-lava.net
Twitter: iamlaz