Clark Nuber PS

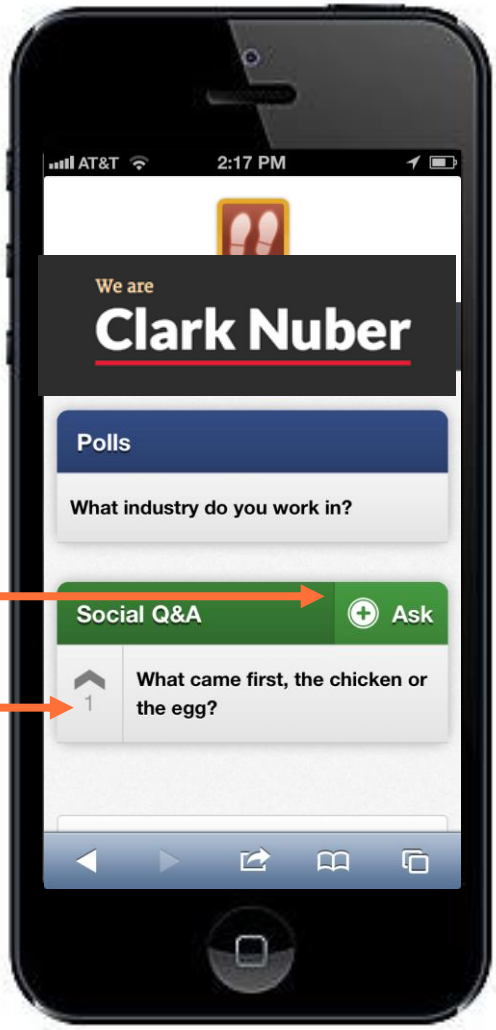
What are the Controller's and CFO's Roles in Data Security?

Reduce Risk by Taking Action

CLARKNUBER.CNF.IO

Ask a Question

Vote for a question



Program Discussion

- Key statistics in cyber security
- Survey questions and results
- Why Controllers and CFOs are getting involved in data security
- Key components in data security and information technology risk management
- Best practices for managing information technology
- Risks and mitigations involved with the use of mobile devices and cloud computing

Key Statistics in Cyber Security

44% OF SMALL BUSINESSES SAY THEY'VE BEEN VICTIMIZED BY A CYBERCRIME OF SOME KIND AT LEAST ONCE.

AVERAGE NEARLY $9,000 EACH TO RECTIFY.

MORE THAN HALF
OF US SMALL BUSINESSES HAVE EXPERIENCED
AT LEAST ONE DATA BREACH.

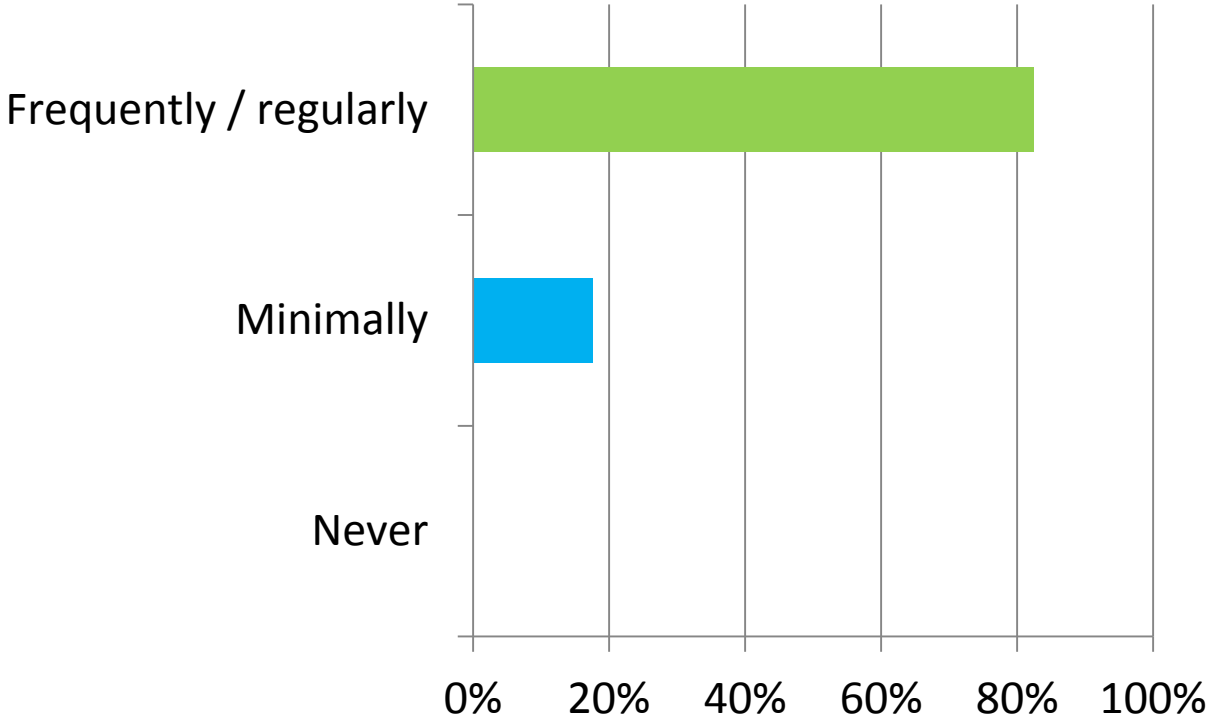
STOLEN
PLATINUM
CREDIT CARDS WITH
HIGH LIMITS
$45 PER RECORD

OTHER CARDS
$1-$10
DEPENDING
ON QUANTITY

BASIC PACKAGE	PREMIUM PACKAGE
Just $3.00	Just $4 to $5.00
> SOCIAL SECURITY NUMBER	> SOCIAL SECURITY NUMBER
	> CREDIT CARD NUMBER WITH EXPIRATION DATE
	> MOTHER'S MAIDEN NAME

Survey Results

How often do you encounter technology-related questions or concerns in your role at the company?



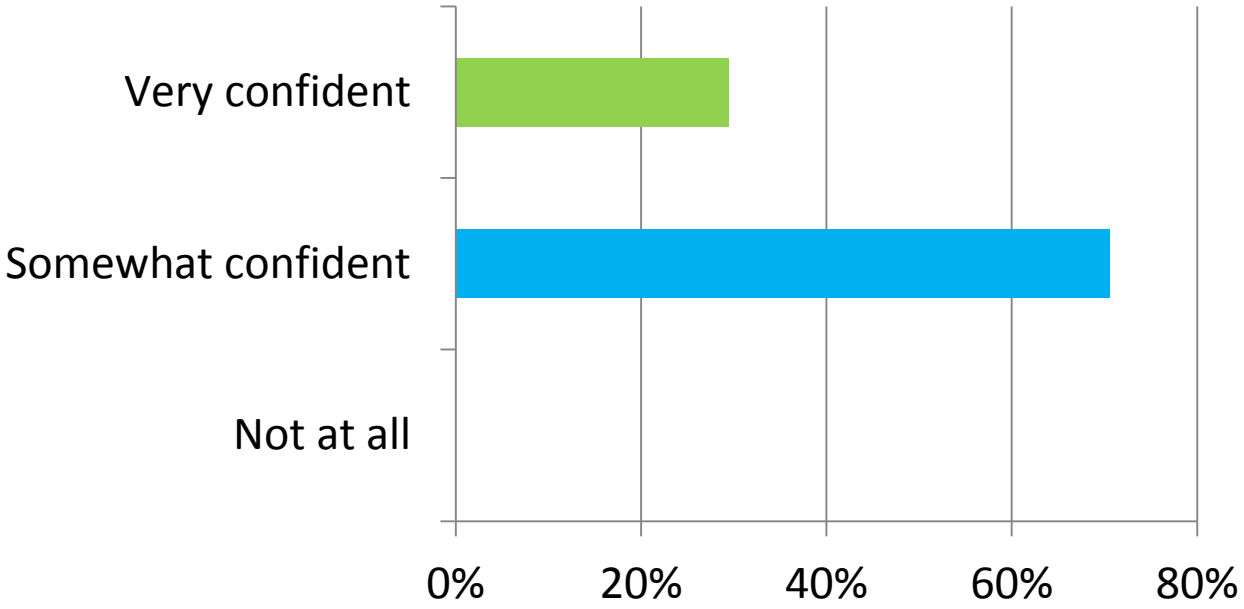
Survey Results

What is your top concern regarding your role in data security?

- Securing the environment
  - Protecting company and investor information
  - Keeping customer and employee information secure
- Having the right people in place
  - Monitoring outside IT firm management
  - Finding resources
- Don’t know what my role is
  - Staying up to date on changing technology / current threats
  - Knowing the right questions to ask
- Losing important data
- Risk management – reputational and fraud

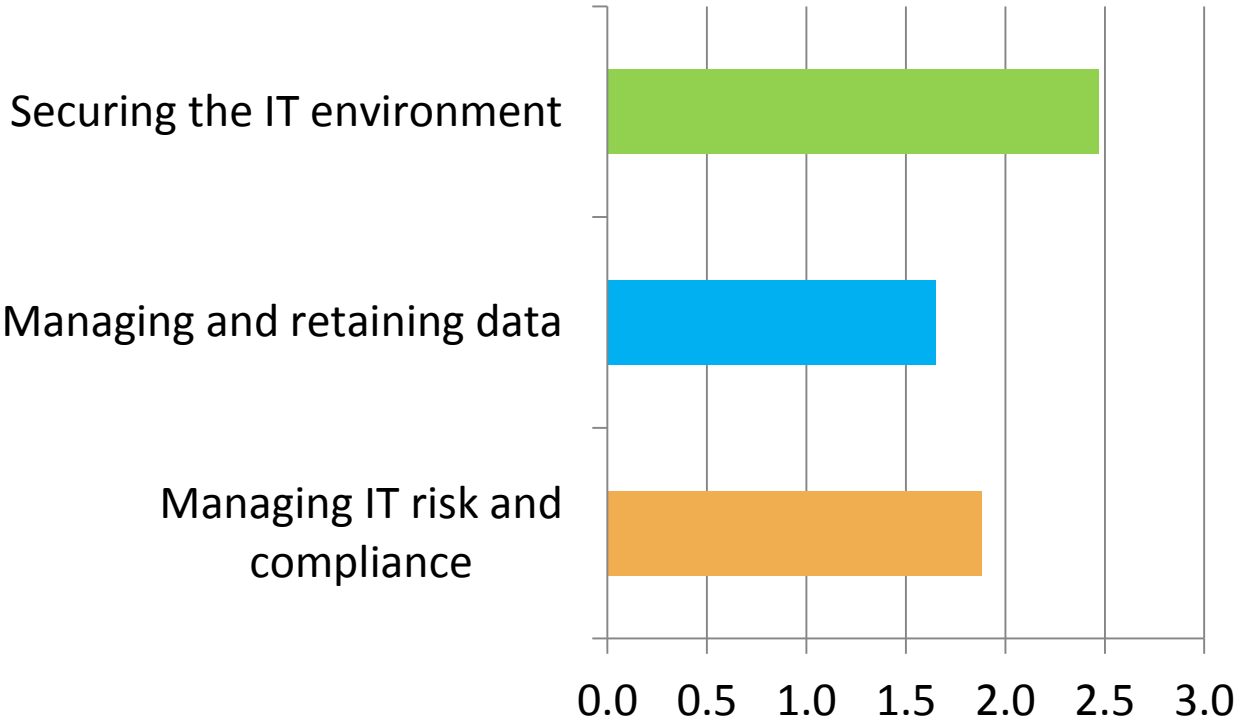
Survey Results

How confident are you in understanding the risk associated with information technology?



Survey Results

What do you see as your top technology initiatives? Ranked from 1 to 3 (1 being top initiative).



Survey Results

TOP 5 Technology Priorities for U.S. Accounting Professionals - AICPA survey results -

1. Securing the IT environment

   8th time at #1 in past 10 surveys
2. Managing and retaining data
3. Ensuring privacy
4. Managing IT risks and compliance
5. Preventing and responding to computer fraud

Controllers and CFOs are Getting Involved

"As overseers of corporate financial performance, Controllers and CFOs must have on their radars the financial impact that results from data breaches."

Not securing data results in 3 serious threats

- Strategic losses
- Regulatory penalties
- Brand reputation damage

The Role of Finance in Data Security

The **"NEW NORMAL"** – a more holistic approach to financial health

- Designing budgets that allocate adequate resources
- Working with IT to design comprehensive data governance plans
- Demanding organization-wide compliance with these plans
- Ensure data supports the company's financial gain while minimizing its role in any loss

Key Components in Data Security

- Perception – Standards and best practices
- Reasonableness – The best fit for your organization
- Balance – Cost, user access, protection complexity
- Data
  - At rest
  - In transit
- Assessment
  - Perimeter
  - Intrusion detection
- Physical, logical, social

Best Practices for Managing IT

- IT as a strategic asset not a cost
- IT Spending levels
- Security
- Governance
- Your company's place on the adoption curve
- Training
- Constituent touch points
- Be a power user

THE FOUR BIG PROBLEMS

1. Sharing your password
2. Clicking on a link that installs malware
3. Plugging in an unknown USB drive
4. Lost or stolen laptop

Risks and Mitigations of Mobile Devices

- Inventory
- Device encryption
- Password enforcement
- Inactivity time out
- Ability to wipe device
- Mobile Device Management (MDM) software

Risks and Mitigations of Cloud Computing

- Build a risk classification of applications and data
- Risk = Threat X vulnerability X consequence
- AICPA SOC 2 report (formerly SAS70, now SSAE16)
- Applications' data locations
- Use reputable data centers
- Develop policies
- Monitor use
- Purchase data breach insurance
- Training

Risks and Mitigations of Cloud Computing

Contract Stage:  Cloud Contract Terms

#1: Data ownership/usage/access
#2: Data Protection Agreement
#3: Meaningful SLAs
#4: Third party access to data
#5: Limitation of liability
#6: Security incident notification
#7: Independent verification
#8: Subcontractor commitments
#9: Terms of use/service changes
#10: Contract suspension/exit

Certifications

Microsoft Cloud Compliance Certifications and Attestations

Regulatory and Compliance Domain	Office 365	Microsoft Dynamics CRM	Microsoft Azure	Microsoft Intune	yammer
CJIS	Yes	No	Yes	No	No
EU Model Clauses	Yes	Yes	Yes	Yes	No
EU Safe Harbor	Yes	Yes	Yes	Yes	Yes
FedRAMP (Moderate)	Yes	No	Yes	No	No
FERPA	Yes	Yes	Yes	N/A	Yes
HIPAA BAA	Yes	Yes	Yes	Yes	No
US Government Cloud	Yes	Yes	Yes	No	No
UK G-Cloud (OFFICIAL)	Yes	Yes	Yes	No	No
ISO 27001:2013 (w/ISO 27018:2014)	Yes	Yes	Yes	Yes	Yes ISO 27001:2005
PCI DSS Level 1	N/A	N/A	Yes	N/A	N/A
SOC 1 Type 2 (SSAE 16 / ISAE 3402)	Yes	Yes	Yes	Yes	No
SOC 2 Type 2 (AT Section 101)	Yes	No	Yes	Yes	No

as of 01/15/15

Service Organization Controls

- SOC 1 – financial reporting
- SOC 2 – security
- SOC 3 – seal and summary report. No carve-outs.
- Type I – point in time
- Type II – functionality over a period of time
- Inclusive vs. carved-out; “subservice provider”
- Three tiered
- User controls – both IT admin and end users
- NDA’s

Questions?

Julie Eisenhauer

jeisenhauer@clarknuber.com

Peter Henley

phenley@clarknuber.com