

BAKER TILLY  
MKM  
CHARTERED  
ACCOUNTANTS

thought leadership ...  
VT  
VALIANT  
TECHNOLOGIES

## Cybercrime Management – Control Perspectives

Dr K Rama Subramaniam

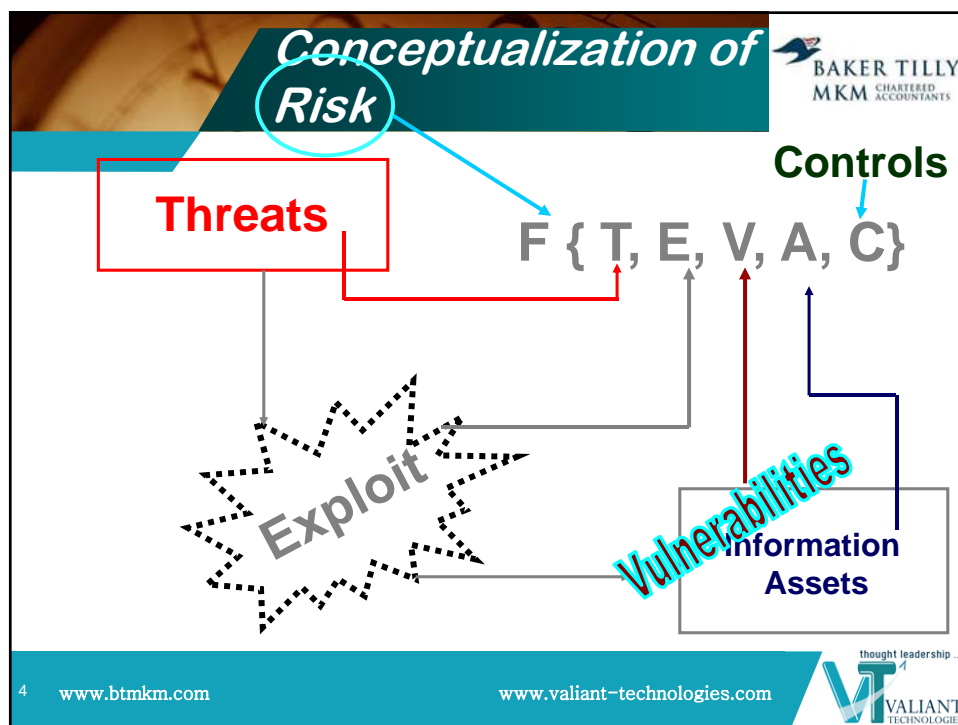
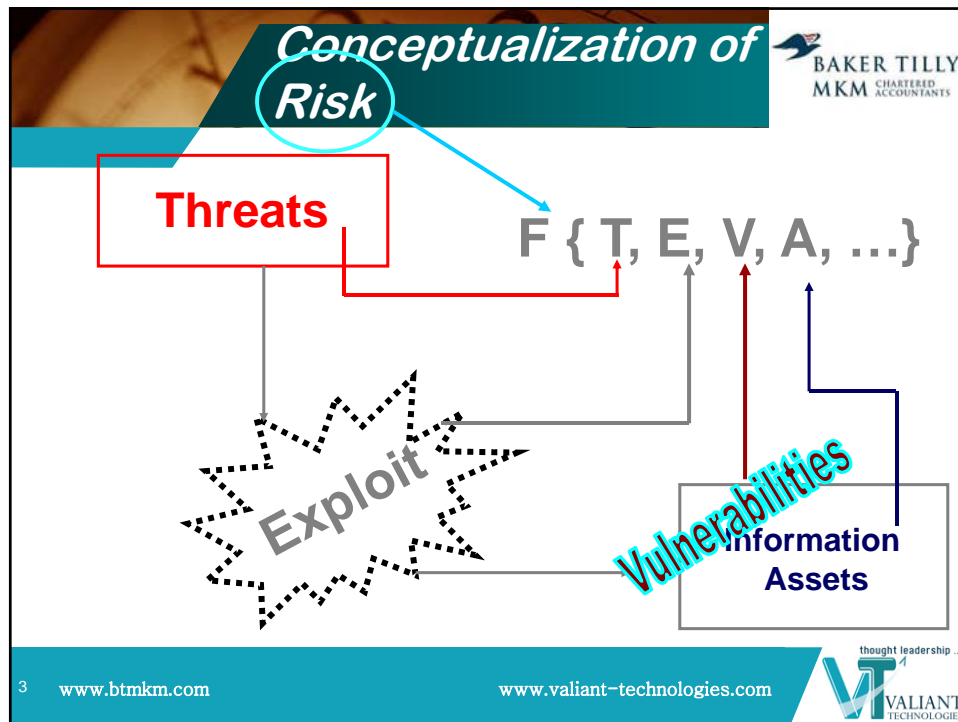
[www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com)

## Agenda

- Protecting corporate information assets – the GRC angle
- Identifying a cybercrime when it has been committed or is about to be perpetrated
- Creating and enforcing a strong control environment
- Response and escalation when you see a cyber infraction
- Why is cybercrime management not merely an IT function
- Implementing and testing the controls for operational assurance and life-cycle assurance

2 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com)

thought leadership ...  
VT  
VALIANT  
TECHNOLOGIES





**Cyber Crimes**

BAKER TILLY  
MKM CHARTERED ACCOUNTANTS

- What is it?
  - Involves use of Computers and often, the Internet too
  - Damages or destroys valuable information asset
  - Compromises the privacy and proprietary controls over information
- What it is not?
  - Crimes that use computers as a better means of communication
  - All that is somehow related to electronics!

5 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) thought leadership ... VALIANT TECHNOLOGIES



BAKER TILLY  
MKM CHARTERED ACCOUNTANTS

**Information is the  
World's new Currency**

- Ralph Basham, Director  
US Secret Service

6 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) thought leadership ... VALIANT TECHNOLOGIES

**We were fighting these....**



**Chen-Ing Hau**  
Author of the CIH virus



**Joseph McElroy**  
Hacked the Fermi lab network



**Benny**  
Ex-29A

7 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) 

**Now, we are fighting these...**



**Jeremy Jaynes**  
Millionaire, and a spammer

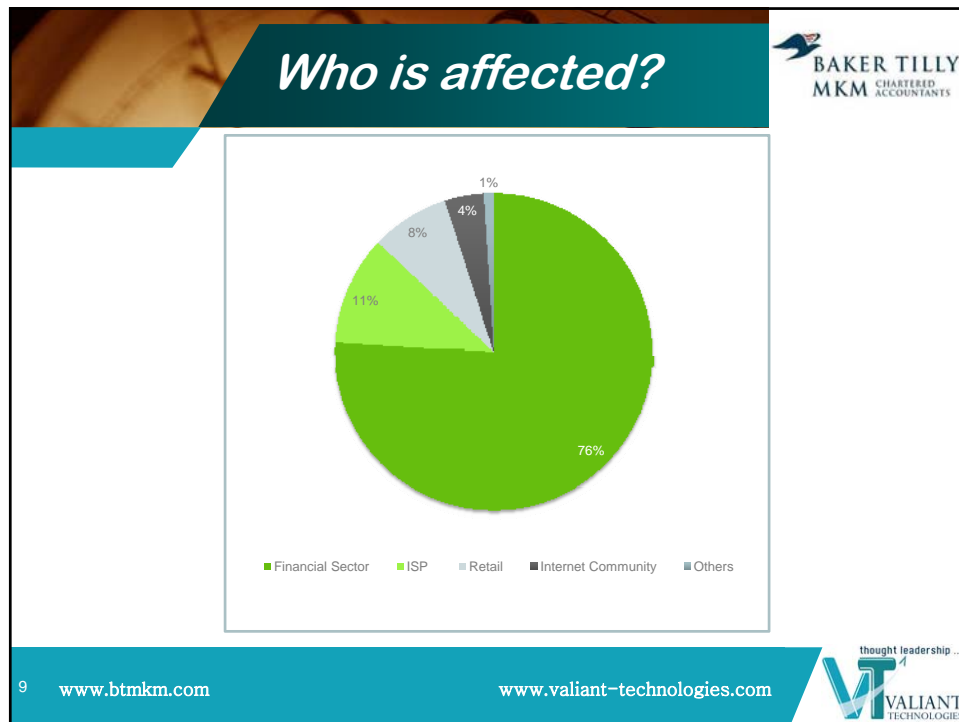


**Jay Echouafni**  
CEO, and a DDoS attacker



**Andrew Schwarmkoff**  
Member of Russian mob, and a phisher

8 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) 



- ### What has changed?
- What has changed?
    - The motivation has changed
    - The rewards have changed
    - The 'goods-on-offer' has increased
  - Other influencers
    - Law enforcement capability has not kept pace
    - Legal system is very slow to recognize these changes
- 10 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com)
- BAKER TILLY MKM CHARTERED ACCOUNTANTS  
thought leadership... VALIANT TECHNOLOGIES

## Who is involved?



<b>Security Illiterate</b>	<ul style="list-style-type: none"><li>• Little knowledge of security</li><li>• Value convenience over security</li></ul>
<b>Gadget Nerds</b>	<ul style="list-style-type: none"><li>• Introduce variety of devices to work PC</li><li>• Move files between computers and devices</li></ul>
<b>Unlawful Residents</b>	<ul style="list-style-type: none"><li>• Don't follow policies and rules</li><li>• Download music, software and videos</li></ul>
<b>Malicious &amp; Disgruntled</b>	<ul style="list-style-type: none"><li>• Marginal of the employees</li><li>• Gain unauthorized access to IT systems</li></ul>

11 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) 

## Cyber criminals are not script kiddies!



- 78% attacks exported user data
- 76% of the attacks used a key stroke logging tool to steal online banking accounts
- 12% of all data breaches that occurred exposed credit card information
- The average cost per incident of a data breach in USA was \$6.7 million
- Lost business amounted to an average of \$4.6 million

12 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) 

## What is on sale?




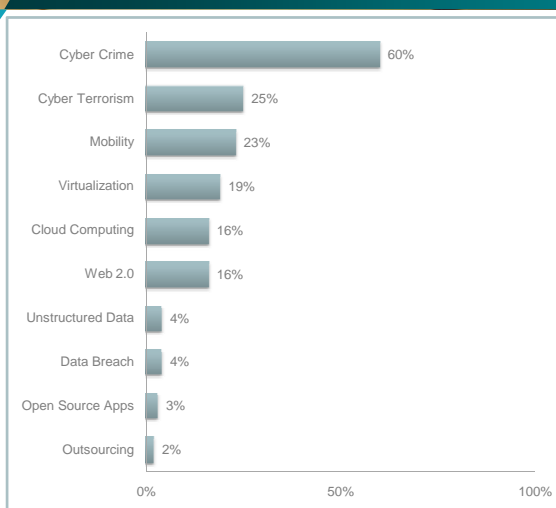
```

NO MORE BOTS . . . JUST REAL USERS . . . :)
12:31 > [redacted] I am a legit drop for items in US , you can trust me 100% , i also can cashout
[redacted] on any id n name just TRY me .
12:31 > [redacted] Scot poste it , , caut persoana care incarca cartele de it . Lasa un id daca
nu sunt !
12:31 > [redacted] I-Selling Cvv2 & Full info (US) - (FR) | Selling Mailist Virgin From Shop
Admin (UK) - (US) - (FR) | Selling Host Hacked | Webmail | Upload All Scam
Page | Upload PHP Mailer | Selling Fast VPN | Selling RDP & VPS & VNC |
Selling Account Socks All Word | I ACCEPT ONLY
12:31 > [redacted] Spam All Banks UK / US * I Can Ship To All Adress ( Europ - USA ) *
Spam Private For Any Client * I Accept Only
12:31 > [redacted] /\ Selling Dumps Track 1 & 2 With Pin /\ Selling Shop Admin US With Big
& Small Daily Order /\ Selling Serial Camfrog & Paltak /\ Selling
Softwre Find Fresh Mailist Perfect /\ Selling Shell C99 /\ Selling Root
/\ - I ACCEPT ONLY
12:31 * [redacted] Chkon [redacted] msr206 [redacted] msg now
12:32 > [redacted] Selling Account SMTP inbox (send to your inbox for test)...also selling US
& UK mailist...selling Host Support Cpanel+ftp...selling SMTP scanner &
SSH Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY [redacted] for serious buyer
[redacted] payment [redacted] only ( RIPPER [redacted] ) !!!
12:32 > [redacted] Set your timers on [redacted] , using => " /timer 0 50 /msg [redacted] your message here
" Enjoy your stay!!
12:32 * [redacted] Selling Fresh Dumps, Cvv2 & Fullz. USA / CAN / UK / Europe. Spammed &
Hacked Shop Admin. Accepting [redacted] + [redacted] + [redacted]
12:32 > [redacted] I Can CASHOUT UK Cvv With POE,
12:32 > [redacted] Selling Account SMTP inbox (send to your inbox for test)...also selling US
& UK mailist...selling Host Support Cpanel+ftp...selling SMTP scanner &
SSH Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY [redacted] for serious buyer
[redacted] payment [redacted] only ( RIPPER [redacted] ) !!!
12:32 * [redacted] free socks http:// [redacted] / user : pas :
12:32 > [redacted] Selling Hacked CPanel, Selling Fresh Mail leads for USA / UK / Uero (MAIL
List), Selling Acces [redacted] Login with verified, Selling [redacted] login with email
acces, Selling IP Sock Any Country ==== Payment [redacted] %
[redacted] ****
    
```


13 www.btmkm.com
www.valiant-technologies.com

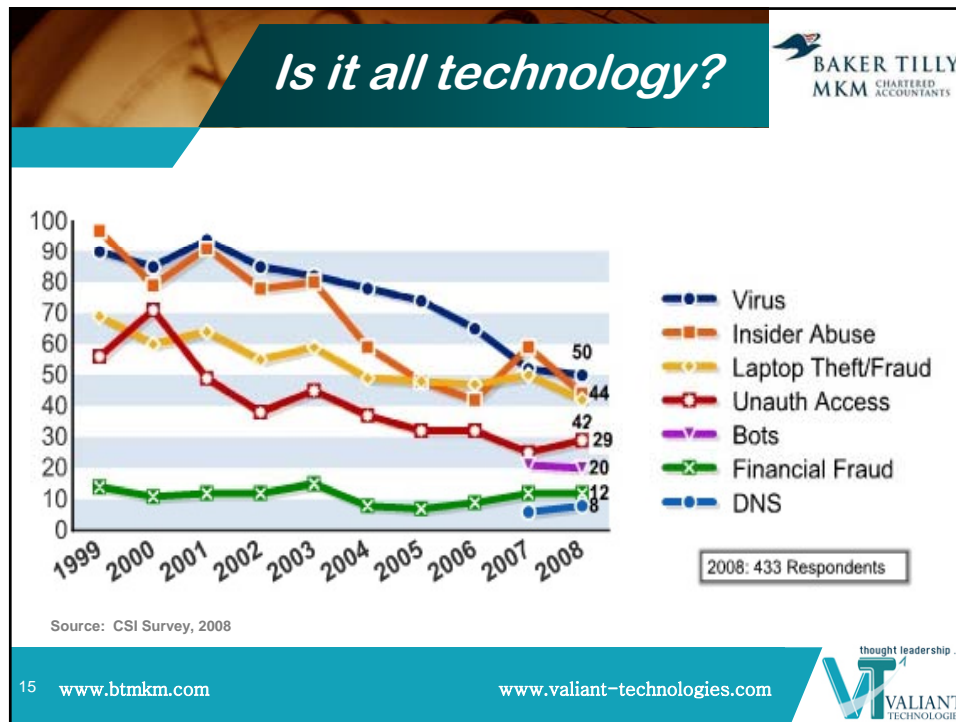

## Security Concerns





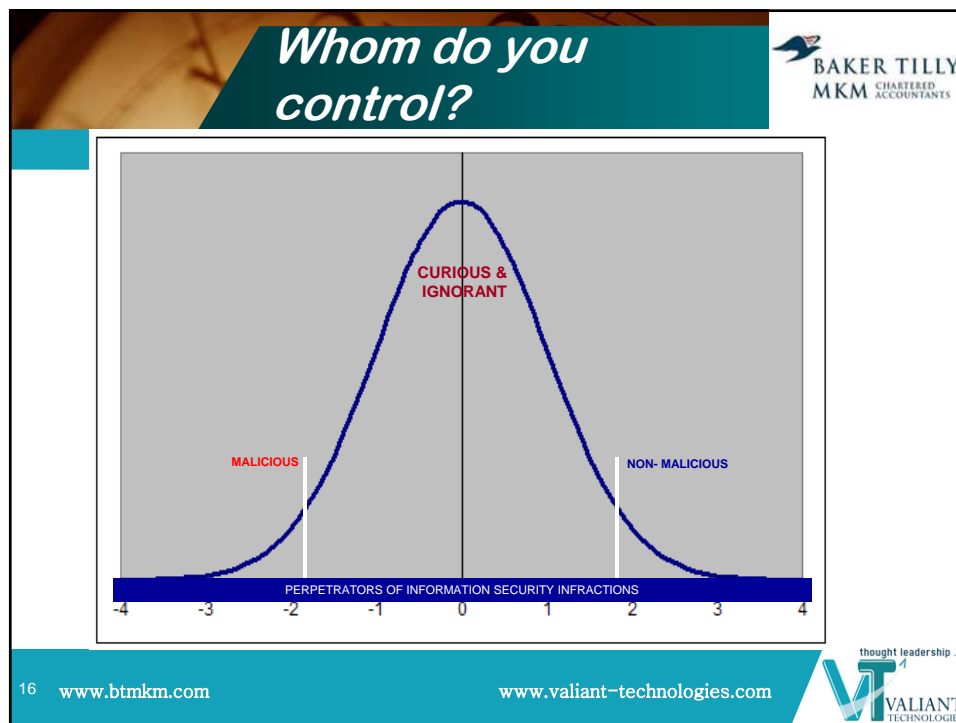
Security Concern	Percentage
Cyber Crime	60%
Cyber Terrorism	25%
Mobility	23%
Virtualization	19%
Cloud Computing	16%
Web 2.0	16%
Unstructured Data	4%
Data Breach	4%
Open Source Apps	3%
Outsourcing	2%

14 www.btmkm.com
www.valiant-technologies.com




15 [www.btmkm.com](http://www.btmkm.com)

[www.valiant-technologies.com](http://www.valiant-technologies.com)



16 [www.btmkm.com](http://www.btmkm.com)

[www.valiant-technologies.com](http://www.valiant-technologies.com)



## Who should handle?



- IT Manager?
- Top Management?
- User Management?
- Corporate Security?
- Audit and Assurance?

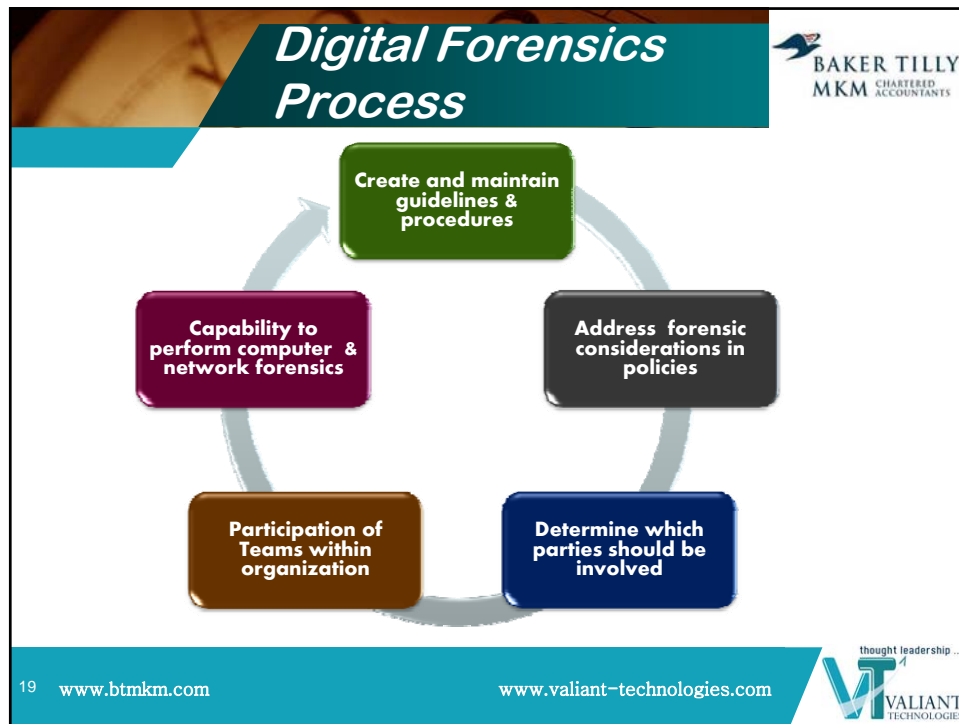
17 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) 

## What do we do?



- Design and Enforce DLP controls
- Increase awareness
- Exemplary action when you identify an infraction
- Good Digital Forensics Mechanism

18 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com) 



- ## What do you assure stakeholders?
- Operational Assurance of Controls
    - Controls are appropriate and relevant
  - Life Cycle Assurance of Controls
    - Controls work the way they were designed to work
- 20 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com)
- BAKER TILLY MKM CHARTERED ACCOUNTANTS  
thought leadership... VALIANT TECHNOLOGIES

BAKER TILLY  
MKM CHARTERED ACCOUNTANTS

***A BRIEF CASE STUDY...***

21 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com)

This slide features a teal header with the Baker Tilly MKM logo. The main content area is white with the text 'A BRIEF CASE STUDY...' in a large, bold, italicized teal font. The footer is teal and contains the slide number '21', two website URLs, and the Valiant Technologies logo.

BAKER TILLY  
MKM CHARTERED ACCOUNTANTS

***THANK YOU***

[rama@btmkm.com](mailto:rama@btmkm.com)

22 [www.btmkm.com](http://www.btmkm.com) [www.valiant-technologies.com](http://www.valiant-technologies.com)

This slide features a teal header with the Baker Tilly MKM logo. The main content area is white with the text 'THANK YOU' in a large, bold, italicized teal font. Below this, the email address 'rama@btmkm.com' is displayed in a smaller teal font. The footer is teal and contains the slide number '22', two website URLs, and the Valiant Technologies logo.