



BDO CYBER FORENSIC LAB

BDO Namibia Half Day Workshop

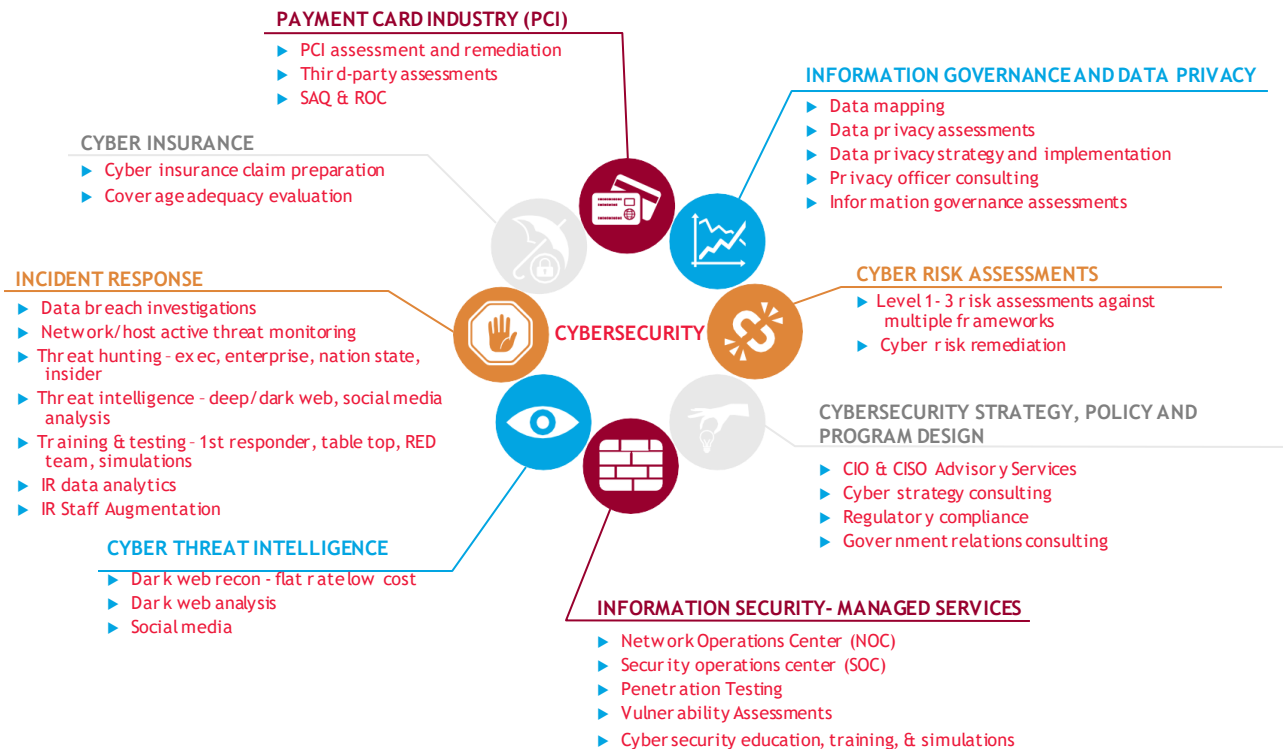
David Cohen

03/04/2019



COMPREHENSIVE CYBERSECURITY PORTFOLIO OF SERVICES

Our full spectrum of services operates in a continual process of risk remediation and security posture improvement.



CYBERSECURITY SERVICE: INFORMATION GOVERNANCE & DATA PRIVACY



Special services

- ▶ Information Governance Assessments
- ▶ Data Privacy Assessments
- ▶ Data Strategy & Implementation Consulting
- ▶ Privacy Officer Consulting
- ▶ Data Mapping
- ▶ Data Privacy Policies Development
- ▶ Global Data Protection Regulation (GDPR) Compliance Consulting



Value proposition

- ▶ Improve information governance
- ▶ Enhance data privacy
- ▶ Optimize the storage, retrieval, use, and disposition of data
- ▶ Reduce data management exposures



Price

- ▶ Information Governance & Data Privacy assessments are fixed priced
- ▶ All other services are time & material (T&M) based upon labor categories required

CYBERSECURITY SERVICE: CYBER RISK ASSESSMENT



Special services

- ▶ Cyber Risk Assessments
 - NIST 800-171 Compliance
 - NYDFS Compliance
 - HIPAA Compliance
 - ISO 27001 Compliance
- ▶ Self Assessment and/or
- ▶ Facilitated Assessment
- ▶ Follow-Up Remediation Services
 - Policy Development
 - Penetration Testing



Value proposition

- ▶ Conduct Risk/Gap Analysis of current information security plans and policies vs. governance and industry standards
- ▶ Provide a timely and cost-effective cyber risk assessment of subcontractors/third parties
- ▶ Identify information security areas requiring improvement



Price

- ▶ Self-Assessment:
 - w/4 hrs. of analysis
- ▶ Facilitated Assessment:
 - Depends upon size & complexity of organization

CYBERSECURITY SERVICE: CYBERSECURITY STRATEGY, POLICY & PROGRAM DESIGN



Special services

- ▶ C-Suite Cyber Advisory Services
- ▶ CIO & CISO strategic business planning
- ▶ Cyber security regulatory compliance consulting
- ▶ Information security organizational design best practices consulting
- ▶ Cyber security policy development
- ▶ Cyber security executive - level education/training seminars



Value proposition

- ▶ Share industry cybersecurity policies, planning, technology, and tools - best practices with company executives
- ▶ Assist corporate senior executives in cybersecurity strategic planning to improve security/data protection
- ▶ Optimize cybersecurity investment
- ▶ Provide Cyber security executive-level education/training



Price

- ▶ Time & Materials (T&M) pricing based upon level of expertise required-range
- ▶ Fixed price for training seminars (depends upon # of attendees & length of seminar)

CYBERSECURITY SERVICE: INFORMATION SECURITY MANAGED SERVICES



Special services

- ▶ Network Operations Center (NOCaS) as a Service
- ▶ SIEM as a Service
- ▶ Security Operations Center (SOC) as a Service
- ▶ Penetration Testing
- ▶ Vulnerability Assessments
- ▶ Cyber security Advanced education, training, and simulations



Value proposition

- ▶ Provide extensive high quality managed security services
- ▶ Allow clients to enhance cybersecurity capabilities at reduce prices vs. in-house
- ▶ Make available state-of-the-art cyber education, training, technology, tools, simulations at affordable prices



Price

- ▶ NOC, SIEM, & SOC managed services are sold fixed price on an annual basis - depending upon the number of users and servers with discounts for multi-year contracts
- ▶ Vulnerability Assessments and Penetration Testing is fixed price on a daily-basis, discounts for longer durations
- ▶ Cybersecurity advanced education, training, & simulations are fixed priced based upon the # of attendees

CYBERSECURITY SERVICE: SOC AS A SERVICE



Special services

- ▶ Network monitoring and detection service
 - Silver - 9 x 5 services
 - Gold - 24 x 7 services
- ▶ Alert analysis and incident response services
- ▶ Analyst services
- ▶ Responder of call (SLA)
- ▶ Cyber hunting (SLA)
- ▶ Incident reporting (SLA)



Value proposition

- ▶ Provide high quality managed Security Operations Center (SOC) services as needed with Silver and Gold options
- ▶ Affordable managed detection and incident response service customized to your Service Level Agreement (SLA) requirements



Price

- ▶ Fixed-price annual services agreement, depends on # of users, network complexity, and SLA requirements
- ▶ Discounts available for multi-year service agreements

CYBERSECURITY SERVICE: SECURITY INCIDENT EVENT MANAGEMENT (SIEM) AS A SERVICE



Special services

- ▶ Security incident log / event collection
- ▶ Event preservation
- ▶ Correlation-based alerts
- ▶ Standard security devices collection
 - Active Directory
 - Firewall
 - Antivirus
- Proxy
- VPN
- Critical servers
- ▶ Selected KPIs per device
- ▶ Analyst services
- ▶ Portal access for forensics and dashboard



Value proposition

- ▶ Provide high quality managed Security Incident Event Management services
- ▶ Timely and affordable
- ▶ Scalable and customized to your SLA requirements



Price

- ▶ Fixed-price annual services agreement, depends upon # of users, devices, and complexity of SLA requirements
- ▶ Discounts available for multi-year service agreements

CYBERSECURITY SERVICE: CYBER ADVANCED EDUCATION, TRAINING, AND SIMULATIONS



Special services

- ▶ Cybersecurity Network Training Simulator (10+ students)
- ▶ Hands-on-Training simulator (max of 3 students)
- ▶ Virtualized Cyber Classroom (up to 30 students)
- ▶ Cyber-Range Global Internet simulator



Value proposition

- ▶ State-of-the-art cyber education and training via advanced simulators
- ▶ Hands-on learning
- ▶ Customizable
- ▶ Very realistic scenarios



Price

- ▶ Fixed-price either per student or per class, depends upon location, customization, and # of students/sessions

CYBERSECURITY SERVICE: MANAGED CLOUD MIGRATION SERVICES



Special services

- ▶ Cloud Services Provider (CSP):
 - AWS, or
 - Microsoft
- ▶ Cloud Migration Services - system integration via InfoReliance or 1901 Group
- ▶ Customized Service Level Agreements (SLAs)



Value proposition

- ▶ Best-in-class Cloud service providers
- ▶ Proven high quality cloud migration services systems integrator
- ▶ Significant cost-savings versus data centers



Price

- ▶ Fixed-price based upon the # of devices, users, and complexity of SLA requirements

CYBERSECURITY SERVICE: CYBER THREAT INTELLIGENCE



Special services

- ▶ Dark Web Recon
- ▶ Dark Web Analysis
- ▶ Social Media Analysis
- ▶ Threat Intelligence gather & Analysis



Value proposition

- ▶ Conduct extensive proactive threat intelligence gathering and analysis to mitigate cyber breach cost impacts
- ▶ Provide post-breach deep dive analysis on actual cyber attacker(s)
- ▶ Reduce the cost of impact of future cyber attacks



Price

- ▶ Sold as a Fixed-Priced-Level-Of-Effort for each service

CYBERSECURITY SERVICE: CYBER INSURANCE



Special services

- ▶ Cybersecurity Insurance Coverage Adequacy Evaluation
- ▶ Cyber Breach Claim Preparation
- ▶ Cyber Breach Claim Evaluation



Value proposition

- ▶ Ensure an organization has adequate cyber liability insurance coverage to protect their information assets
- ▶ Prepare detailed cyber breach claims in a timely and cost-effective manner to maximize damage reimbursement
- ▶ Evaluate cyber breach claims for adequacy



Price

- ▶ Sold as a Fixed-Priced-Level-Of-Effort for each service



BDO CYBER TRAINING ACADEMY

BDO Namibia Half Day Workshop

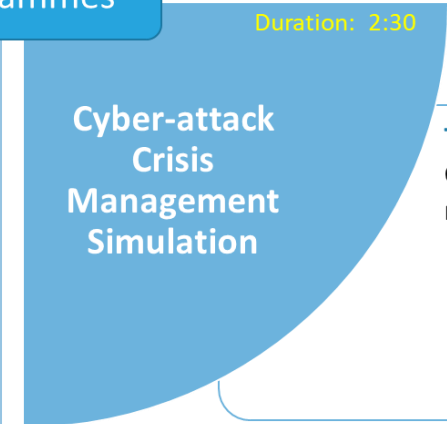
David Cohen

04 April 2019

Title: Meet the Hacker
Classroom training & video linkup for remote destinations
All Staff using an electronic devise connected to the internet.



Programmes



Title: How Hackers think
IT division (in depth training)

- IT department
- Network administrators
- Security specialists



Title: Hackers Mean Business
Key departments:

- HR
- Finance Department
- Procurement
- First line support staff such as call centre staff



Title: How to deal with a hack
C-Level executives and Board members



CYBER CAMPAIGN



Analytics and Reports



Passports



Knowledge Assessment



2 min Training Videos



Posters



David Cohen
CISO

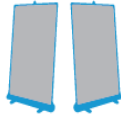
INFORMATION SECURITY & CYBER DEFENSE

Imperial
logistics

Signatures



Screen saver



Rollup Banners



Digital Banners



Teaser/Emailer



Warnings



Officer Badges



Cyber Magazine



Infographics

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
		Monthly Newsletter				Monthly Newsletter				Monthly Newsletter	
Cyber Magazine				Cyber Magazine				Cyber Magazine			
	Infographics		Infographics				Infographics		Infographics		
		Video			Video			Video			
Poster A3 Design				Poster A3 Design					Poster A3 Design		
Pull Up Banners					Pull Up Banners						
	Email Set up										
	Digital Banners					Digital Banners					
					Passports						
		Screensaver						Screensaver			
	Social Engineering										
Phishing Attack								Phishing Attack			

Cyber Awareness

Announcements

Course Introduction



Meet the Hacker



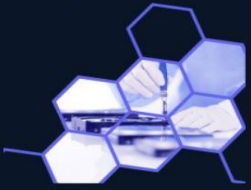
Social Engineering



Physical Security



Malware & Ransomware



Personal Security



Mobile Security
The internet of things



P***word
Protec***n



Real Examples

Navigation

- Dashboard
- Site home
- Site pages
- My courses
 - Cyber Demo Course
 - Participants
 - Badges
 - Competencies
 - Grades
 - Cyber Awareness - Demo
 - Demo Course - Introduction
 - Topic 2 - Social Engineering
 - Topic 3 - Physical Security
 - Topic 4 - Malware & Ransomware
 - Knowledge Check
- Courses
 - Cyber Awareness

Completion Progress



Table of contents

General

Grades:

		Cyber Demo Course				
Surname	First name	Email address	Knowledge Quiz	Meet Bob!	KC 4	Course total
	Heinz Benninghoff	heinz@bluerooster.co.za	5.31	6.67	2.50	14.48
	Kevin Bracegirdle	kevin@bluerooster.co.za	2.19	6.67	10.00	18.85
	David Cohen	david.cohen@checkmark.co.za	-	-	-	-
	Rudi Dicks	rudi.dicks@checkmark.co.za	-	-	-	-
	Reinet Herbst	Reinet@bluerooster.co.za	7.81	6.67	7.50	21.98
	Linda Ingram	linda@theeducationscene.com	-	-	-	-
	Lelanie Judeel	lelanie@bluerooster.co.za	-	-	-	-
	Carien Rooseboom	carien@bluerooster.co.za	7.50	-	0.00	7.50
	Wilmari van der Merwe	wilmari@bluerooster.co.za	6.98	3.33	10.00	20.31
	Melissa van der Walt	melissa@bluerooster.co.za	-	-	-	-
	Michelle van Schalkwyk	michelle@bluerooster.co.za	6.35	6.67	5.00	18.02
Overall average			6.02	6.00	5.83	16.86

Table of contents



Cyber Awareness - Demo

- 1 Demo Course - Introduction
- 2 Topic 2 - Social Engineering
- 3 Topic 3 - Physical Security
- 4 Topic 4 - Malware & Ransomware
- 5 Knowledge Check

Completion Progress



NOW


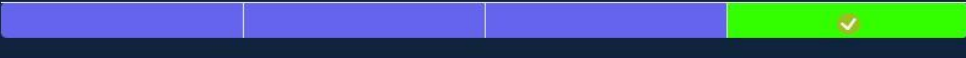

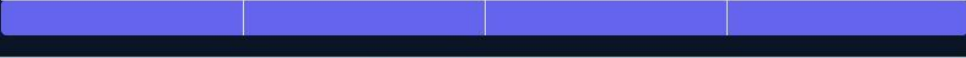

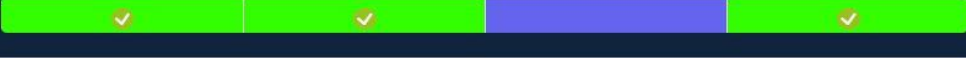
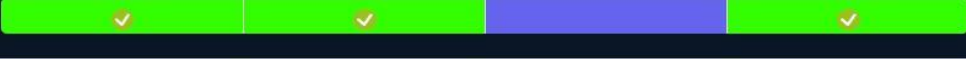





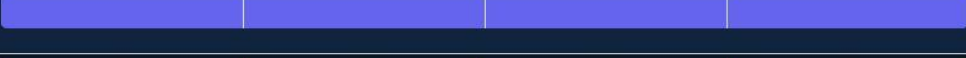




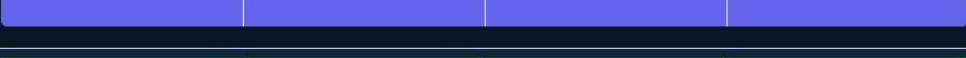




Progress: 100%



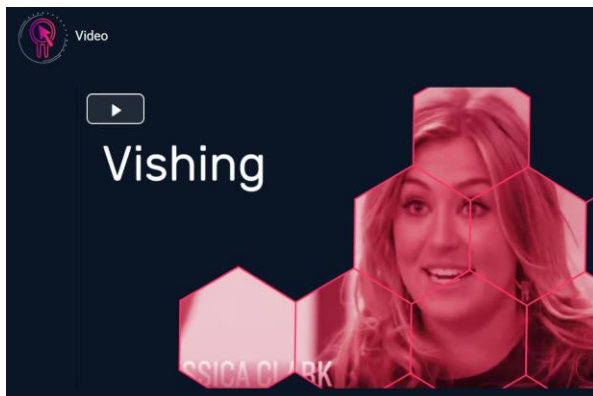
Knowledge Quiz
Completed

Overview of students

First name / Surname	Last in course	Completion Progress				Progress
 Carien Rooseboom	Tuesday, 26 March 2019, 10:59 AM					25%
 David Cohen	Never					0%
 Heinz Benninghoff	Friday, 29 March 2019, 12:24 PM					75%
 Kevin Bracegirdle	Friday, 29 March 2019, 12:12 PM					75%
 Lelanie Judeel	Tuesday, 26 March 2019, 9:29 AM					0%
 Linda Ingram	Never					0%
 Melissa van der Walt	Monday, 25 March 2019, 4:00 PM					0%
 Michelle van Schalkwyk	Friday, 29 March 2019, 12:34 PM					100%
 Reinet Herbst	Friday, 29 March 2019, 12:29 PM					100%
 Rudi Dicks	Never					0%
 Wilmari van der Merwe	Friday, 29 March 2019, 1:17 PM					100%

Course Activities

1. Video Content
2. Infographics
3. Interactivity
4. Hotspot activities
5. Interactive Videos:
6. Branching Scenarios
7. Knowledge Check
8. Final Assessment

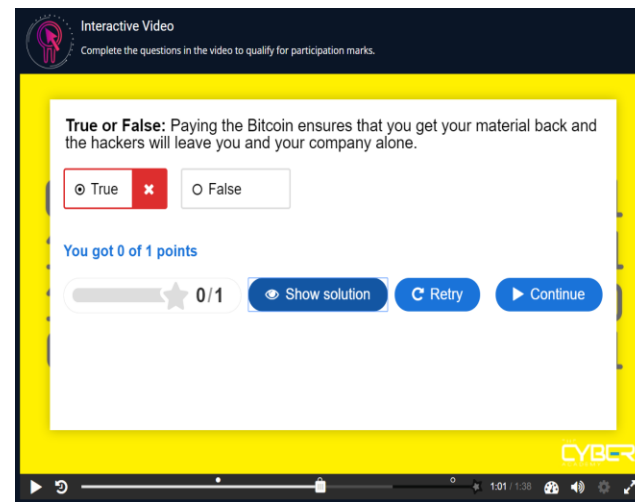
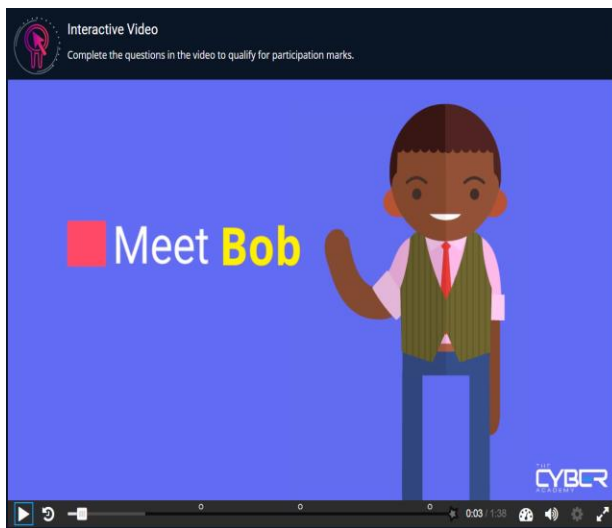


TIPS: Protect yourself against a whaling scam

1. Never rush to pay a client urgently, you are the only one who can lose.

STOP > THINK > PROCEED

2. Insist on compiling company policies and procedures for payments and financial processes. These documents will protect you.
3. Always call the client and confirm the banking details telephonically.
4. Try to get verbal confirmation from senior managers around urgent payments.



1. Branching Scenarios


CYBER

Do we pay the ransom to unlock our own data so that the business can continue to operate?

Yes

No

Click on **Yes** or **No** to select your decision.




CYBER

To **Pay** ... or **NOT** to Pay?

You are the manager of your company and have some very difficult decisions to make.

How would you solve this problem?

NEXT >>



Takeaway TIPS:

Click on the numbers to see all tips: [1](#) [2](#) [3](#) [4](#) [5](#)

4


Don't pay should be the **default position** but it's **not always this simple**. There are many factors that determine which outcome is correct for you. Let's imagine the attackers also encrypted your backups and you have no access to your data. The

Scroll to read more

[<<BACK to Question](#)

CYBER

END>>



restore@amazons.com

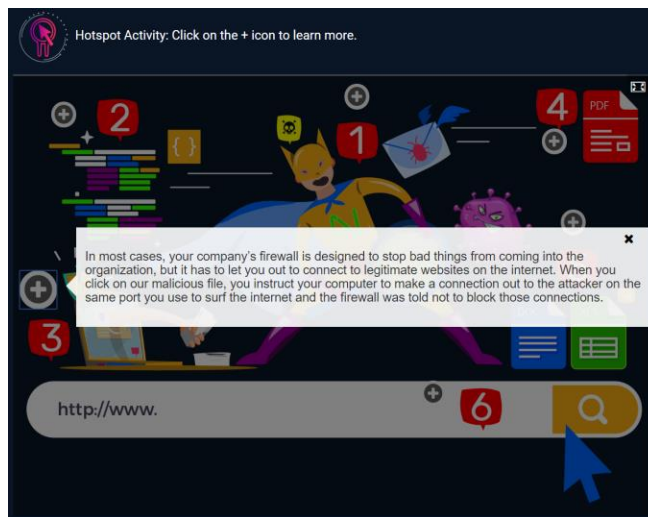
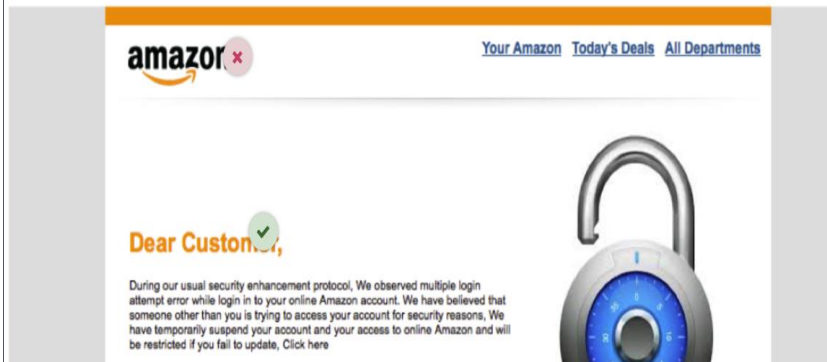
To: mduinn@pinsec.com


Reply-To: restore@amazons.com ✓

Amazon : Restore Your Online Account Access


November 11, 2013 5:05 AM


[Hide Details](#)





Knowledge Check



 Knowledge Check 4

1 / 5

Fill in the missing words

software allows you a copy of the program that either has partial or full functionality enabled to allow you to try before you buy. is software that requires no license to use. The people who developed the software are giving it away.

My courses > Cyber Demo Course > Knowledge Check > Knowledge Quiz > Preview

Question 5

What happens when you open a virus file?

Not yet answered

Marked out of 1.00

Flag question

Edit question

Select one:

- a. The hacker never gain access to your machine, because of the anti-virus or firewall your company has in place.
- b. The hacker almost always gain full access to your machine, regardless of what anti-virus or firewall your company has in place.

Summary of your previous attempts

Attempt	State	Marks / 16.00	Grade / 10.00	Review
1	Finished Submitted Tuesday, 26 March 2019, 10:38 AM	11.17	6.98	Review

Highest grade: 6.98 / 10.00.

Quiz navigation

