THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING

RSM

TOMORROW’S RSM

THE RESPONSIBILITY OF C-LEVEL MANAGERS TO PREVENT CYBER-ATTACKS AND HOW TO REDUCE CYBER SECURITY THREATS

RSM

RSM POLAND

The speaker

Sebastian Goschorski, an experienced financial officer, certified accountant and a Partner at RSM Poland responsible for business development, in relations between Poland and China. He has a 15 years of experience in heading and managing accounting, finance, tax and HR & payroll departments, as well as designing and implementing company development strategies.

EUROPOL'S 2019 CYBERCRIME REPORT

Europol's 2019 cybercrime report provides insights into emerging threats and key developments.

1. Ransomware.
2. DDoS attacks.
3. Data overload in fighting child sexual exploitation material.
4. Self-generated explicit material.
5. Smart cities.
6. Law enforcement is increasingly responding to attacks on critical infrastructure.
7. The Darknet is becoming more fragmented.
8. Blockchain marketplaces.
9. Business email compromise.
10. EU law enforcement emergency response protocol.

https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene

SOME SCARY CYBERSECURITY STATISTICS FOR 2020

1. The US had a $15 billion cybersecurity budget for 2019, but in 2021, the cybersecurity damage is expected to reach $6 trillion.
2. Not so surprising, given that 50% of users would click on a link from unknown sender…
3. …and that the majority of IoT devices reduce the overall security.
4. 43% of cyber attacks are aimed at small business.
5. 58% of malware attacks are directed at small business.
6. Still, financial companies pay the most – on average, $18.3 million per surveyed company.
7. 90% of the CIOs state their cybersecurity budget is spent inefficiently.

https://hostingtribunal.com/blog/cybersecurity-statistics/#gref

The speakers

Shlomy Benny – BA, CPA CISA Leader IT and Cyber Security department. Mr. Benny has over 15 years of experience in management, combined with system and information security. Ms. Benny has vast experience as an advisor to clients in Israel and abroad in the pharmacy, E-commerce, finance, insurance, banking industries and etc.

Boris Kogan – BSc, CISSP, CISA,CISM Information Security and Cyber Architect, IT and Cyber Security department. Mr. Kogan has over 20 years of experience in system and information & Cyber Security (e-commerce, banks channels). Mr. Boris had served as a senior consultant for Isracart (Credit company), Leumi card (VISA Israel), Discount bank and more.

RSM ISRAEL

- RSM Israel is one of Israel's Top-Ten Full-Service accounting and consulting firms and a member of the RSM network, the 6th largest firm in the world.
- RSM Israel Established in 1978 and located in Tel-Aviv and Haifa.
- Together with 15 partners and about 160 employees, the firm serves about 2,500 private, public and government sector clients.
- Our services includes: audit & assurance, taxation services, internal audit & risk management, advisory services, Cyber Security, IT audit and advisory, corporate finance services, professional practice and trust management.

RSM ISRAEL - CYBER SECURITY DEPARTMENT

- RSM Israel Cyber security Department offers many services in Cyber like: Cyber Risk Assessments (Survey and Penetration tests), Cyber security training, preparing organizations for regulation, etc.

- Our consulting team has gained international experience focusing on Cyber Security, privacy regulation compliance, IT Audit, IT & Cyber Risk Management.

- RSM Poland and RSM Israel jointly provide advanced Cyber Security services.

What is the responsibility of C-level and senior management to prevent Cyber attacks?

CYBER-ATTACKS ARE THE PRICE WE PAY FOR CONDUCTING BUSINESS IN THE AGE OF DIGITAL ECONOMY

CYBER DAMAGE

Direct costs	Indirect costs
Handling of cyber event • protection to victims • legal, communications and similar steps	Damage to reputation
Returning computer system to its pre-attack state	Loss of trust (customers, vendors)
Loss of expected profits	Increase in cyber insurance premiums
Loss of manpower	Other costs (not easy to quantify)
Loss of business information	
Damage to actual operations	

1

Has the entity set out an information security procedure that will maintain information confidentiality?

PRACTICAL RECOMMENDATIONS

2

Does the entity have an ongoing control policy regarding the information security systems and its exposure to cyber threats?

PRACTICAL RECOMMENDATIONS

3

Is there an organizational response policy to contend with cyber events and data leakage?

PRACTICAL RECOMMENDATIONS

4

Are the employees of the entity trained, to the extent possible, to protect the information security of the entity?

PRACTICAL RECOMMENDATIONS

5

Does the entity strictly enforce information security principles also in its dealings with third party vendors?

PRACTICAL RECOMMENDATIONS

SUMMARY

- C-level and senior management are responsible to take an active role in setting and implementing an organizational cyber protection policy.

- C-level and senior management must be optimally prepared for cyber-attacks or physical security breaches.

- We recommend that companies and other organizations formulate orderly work procedures in consultation with a professional with expertise in the field of cyber risks.

SEVEN SIMPLE TIPS TO REDUCE CYBER SECURITY THREATS

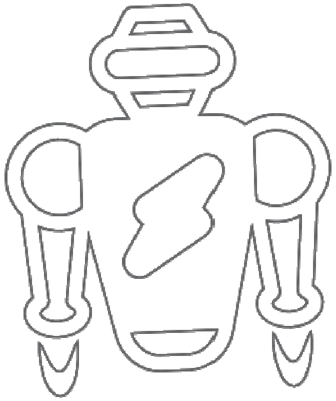
BORIS KOGAN - BSC, CISSP, CISA,CISM

RSM

SEVEN SIMPLE TIPS TO REDUCE CYBER SECURITY THREATS

1. Limit access permissions – currently, it is recommended to limit the number of user access permissions to a minimum required for their work, regarding both the corporate network and software.

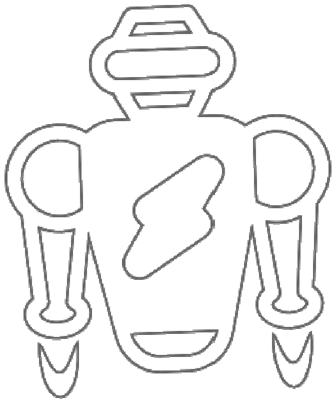
2. Limiting network access via Firewall – it is recommended to review Firewall rules, limit the access to corporate network to a minimum. For example, it is advisable to set countries and regions that are allowed to connect to the organization.



SEVEN SIMPLE TIPS TO REDUCE CYBER SECURITY THREATS

3. Updating the operation systems and software versions – it is recommended to update organizational operation systems and software to the latest versions, since most of newer versions are offered to organizations due to security breaches detected in older versions.

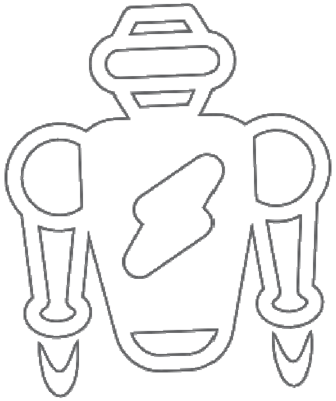
4. Restricting command line Access – (such as Power Shell) must be restricted so that scripts from unknown sources or from another computer cannot be run.



SEVEN SIMPLE TIPS TO REDUCE CYBER SECURITY THREATS

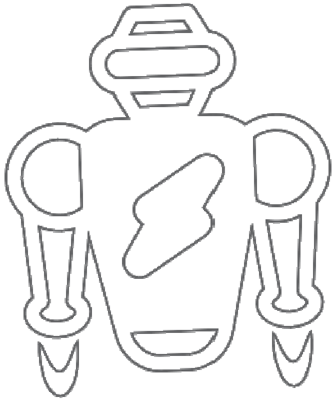
5. Sharpen Awareness of phishing attempts – all employees must be made aware of phishing attempts made via the various media channels (private and organizational). Employees must also understand the importance of updating IT staff or management with any suspicion of such experience.

6. 3rd party remote access – review all 3rd party suppliers that are able to connect to company assets.



SEVEN SIMPLE TIPS TO REDUCE CYBER SECURITY THREATS

7. Automatic updates to information security software – Push an automatic version update for any information security software which is installed on the employee computer (e.g antivirus and firewall) at any connection to the organization network.



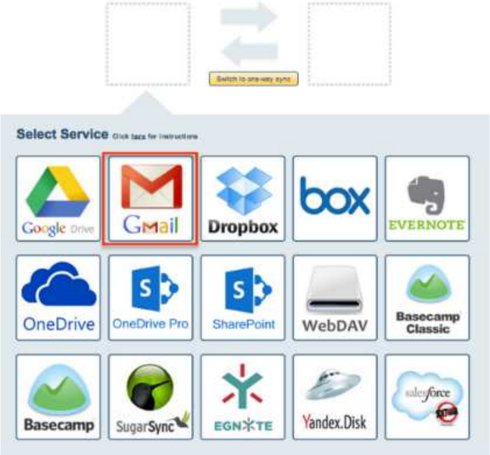
ARE CLOUD SERVICES SAFE?

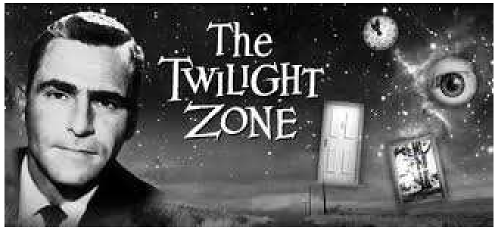
Boris Kogan – BSc, CISSP, CISA, CISM

MAYBE...

YOU ARE ALREADY THERE!

- Even if you don’t use cloud services, your employees most likely do or will – create a cloud use policy.
- Be prepared – evaluate corporate applications, business processes, and data according to their value to the organization and risk when deployed wholly or partially in the cloud.





THE THREE MODELS OF CLOUD COMPUTING

- Infrastructure-as-a-service (IaaS)
- Platform-as-a-service (PaaS)
- Software-as-a-service (SaaS)

***Please choose wisely

Start cloud use with low-risk, non-core functions until your organization gets a grip on the security landscape.

CONSIDERATION FOR SECURITY PRODUCTS

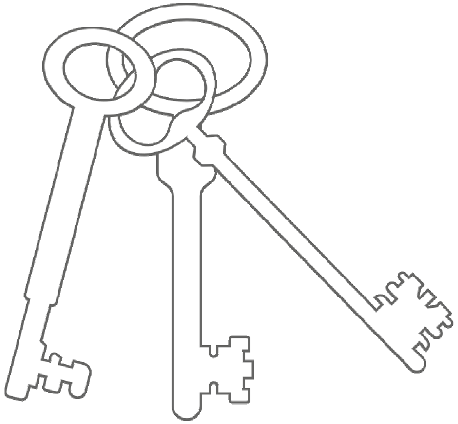
- Align your cloud architecture to company information security policy.
- Install proper firewalls – access rules are not enough.
- Create proper segmentation and DMZs.
- Install AV and WAF for internet facing application.
- Seek DDOS protection from your cloud provider.
- Perform Cryptographic Keys Management
- Malware can be in the cloud as well.

DEVOPS – THE NEW KID ON THE BLOCK

- Make sure you train your DevOps on security – remember that the R&D teams working on IT are not primarily concerned with security.
- Provide proper access and control access using secure methods such as VPN.
- Secure your IP and code even in the cloud – Implement a secure development life cycle.

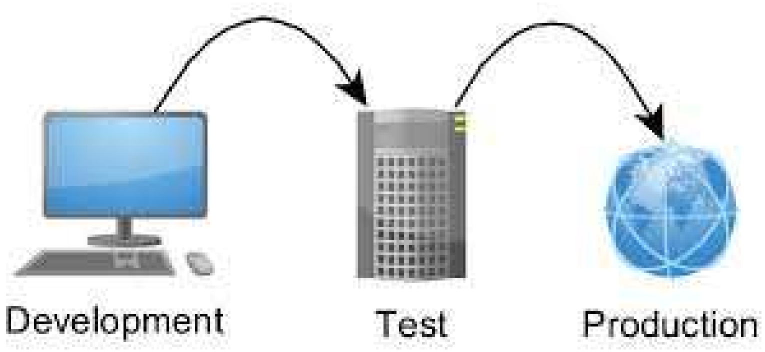
KEYS TO THE KINGDOM

- Be vigilant about access control to administration platform of the cloud – don’t leave accounts of retired users.
- Strive to Integrate your cloud environments into your corporate AD or LDAP centralized authentication model and enforce two-factor authentication where possible.



TEST AND PRODUCTION

- Make sure to separate Production and Test in the cloud.
- Do not make shortcuts – do not transfer your development cloud to production without sanitation.
- Do not test software in the cloud using live or sensitive corporate or customer information.



THIRD PARTY AND OPEN SOURCE PRODUCTS

- Perform patch management for all your cloud services (OS, applications etc.) and test all updates to confirm that they do not damage or create vulnerabilities before implementation into your live environment.
- Evaluate open source products such as Dokers that you implement on the cloud as if they were in your Data center.

3rd

PARTY

SHARING IS CARING

- Understand how much the Environment / Infrastructure Is shared with other clients
- Is it just infrastructure – firewalls, servers?
- Are you sharing everything and the only segregation of data is in programming logic?

BACKUP’S

- Even if you are on the cloud make sure that you have proper backups frequency, storage.
- Your cloud backups should be correlated with your BCP plan.

LOGS AND SECURITY AUDITS

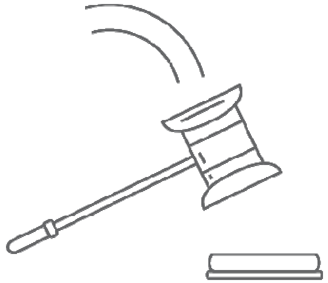
- Log reviews should be an essential component of your organizations security practice – log data is essential for monitoring for malicious activity and forensic investigation.
- Perform security audits and controlled vulnerabilities scans.
- Perform Application Penetration tests and code reviews.

CLOUD OWNER AND SECURITY POINT OF CONTACT

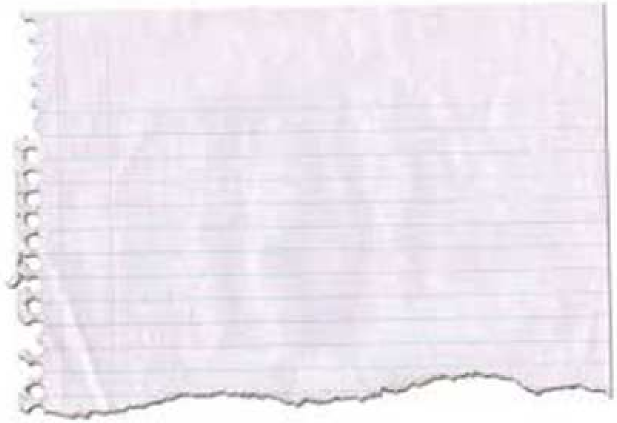
- Make sure to appoint an internal cloud owner – this person will be responsible for managing the security-related requests and problems that could happen.
- Educate your cloud owners about security – phishing, account takeover.
- Monitor your cloud provider bills.

LEGAL AND COMPLIANCE

- Don’t go solo - Make sure that you involve your legal department and Identify where the Solution Data Center(s) Will Be to Meet Local Legal Particularities and regulations and examine your Cloud provider SLA.
- A cloud services provider may occasionally be legally required to deliver information, which may vary according to the laws of each country.
- Understand the role and responsibilities of cloud facilitators (sub lease).
- Even if your cloud provider is certified (ISO, PCIDSS) it does not mean that if you put your data in you will be compliant as well!



- Remember that the cloud is like a blank paper – it will bear anything.
- But like a paper it can be shredded or sometimes land on some one else's desk.



TOMORROW'S RSM

For further information and private on-line meeting please contact:

Shlomy Benny

C.P.A (Isr), Partner, Leader IT and Cyber Security department

E: shlomyb@rsmisrael.co.il

T: +972 50 74 74 177

Tali Gadi

MBA, Marketing & Business Development Director

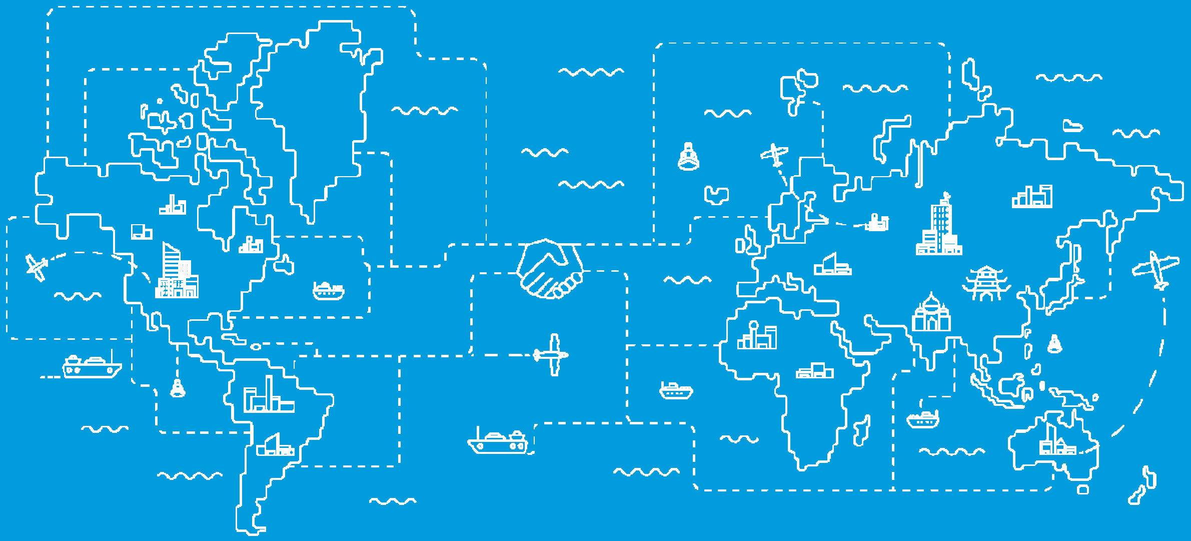
E: Tali@rsmisrael.co.il

T: +972 50 626 0606

RSM

THANK YOU FOR YOUR TIME AND ATTENTION

RSM



Collaboration. Understanding. Ideas and insight.

RSM