Cyber security is a self defense system.
Cyber security is not a technology.
It's an attitude.

Standards vs Hackers and Lawmakers

Michael Petrov
CEO

Digital Edge

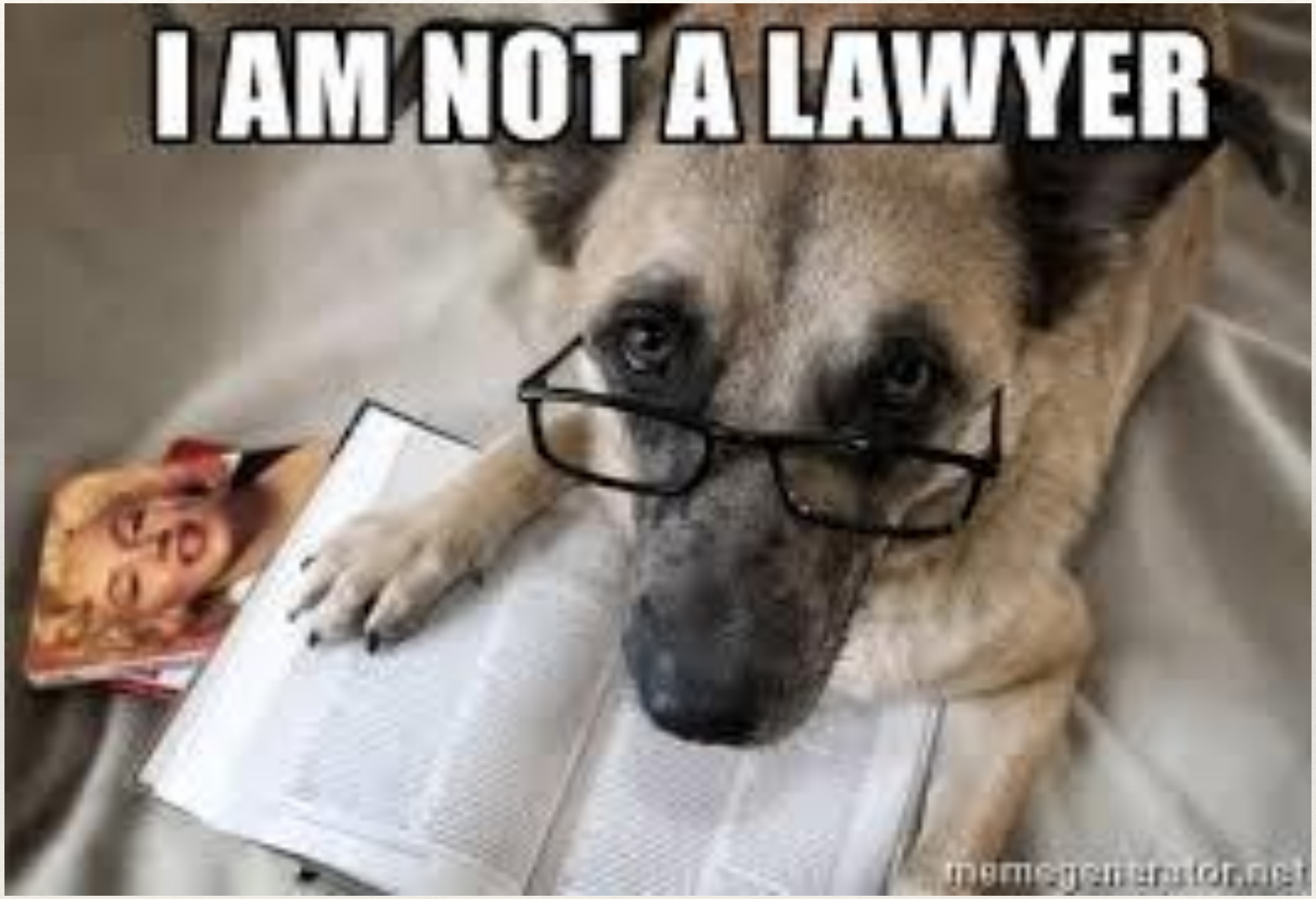
ISACA
Trust in, and value from, information systems

Agenda – Day 1

- Introduction
- Who are the bad guys
- Are you smart enough?
- What Cybersecurity Standards are and what they are not
- Comparison
- Selecting the right framework

Who?

Laws, Regulations, Frameworks, Standards



Under Attack – 2 advisories

Who are the bad guys?

Laws

- Federal Information Security Management Act (FISMA)
- Children's Online Privacy Protection Act (COPPA)
- Computer Fraud and Abuse Act (CFAA)
- Health Insurance Portability and Accountability Act (HIPAA)
- California Online Privacy Protection Act
- New York State SHIELD Act
- Individual State Requirements for Notification
- NYS DFS 500
- GDPR

Regulations

- Regulation S-P (17 CFR §248.30), which requires firms to adopt written policies and procedures to protect customer information against cyber-attacks and other forms of unauthorized access.
- Regulation S-ID (17 CFR §248.201-202), which outlines a firm's duties regarding the detection, prevention, and mitigation of identity theft.
- The Securities Exchange Act of 1934 (17 CFR §240.17a-4(f)), which requires firms to preserve electronically stored records in a non-rewriteable, non-erasable format.
- PCI
- FTC Health Breach Notification Rule
- FTC GLB Safeguard Rule

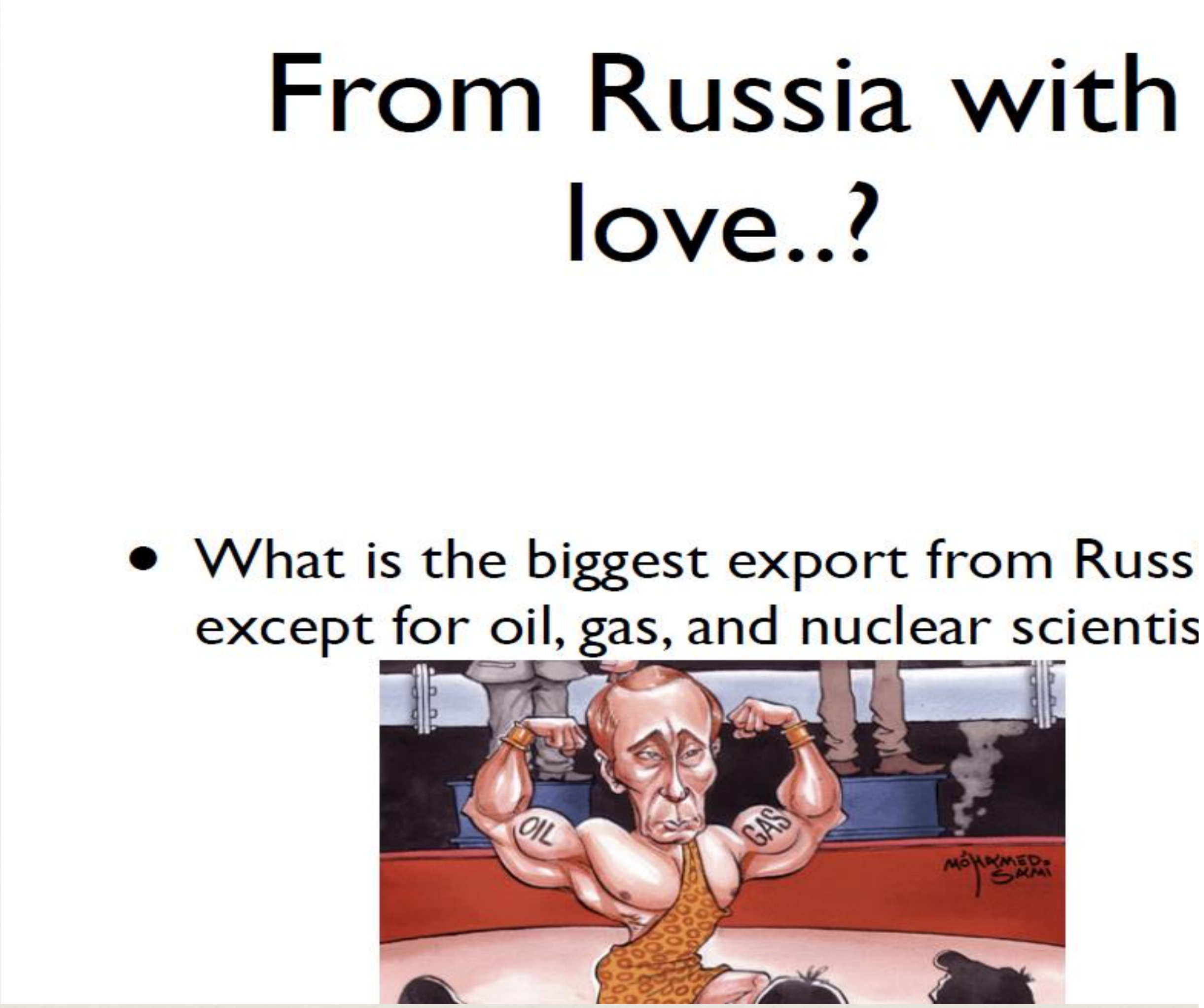
Case Study

XYX Inc. laws application

- FISMA - government contracts?
- Medical? HIPAA
  - Only clinics, insurance, claims
- Children? COPPA?
- GDPR
  - Is EU, Market to EU, trace EU residents (cookies)
- State laws for breach notifications

Who are the bad guys?

Who are the hackers?



From Russia with love..?

- What is the biggest export from Russ except for oil, gas, and nuclear scientis

-Malware -

Stuff that lives in your PC
Against your will :)

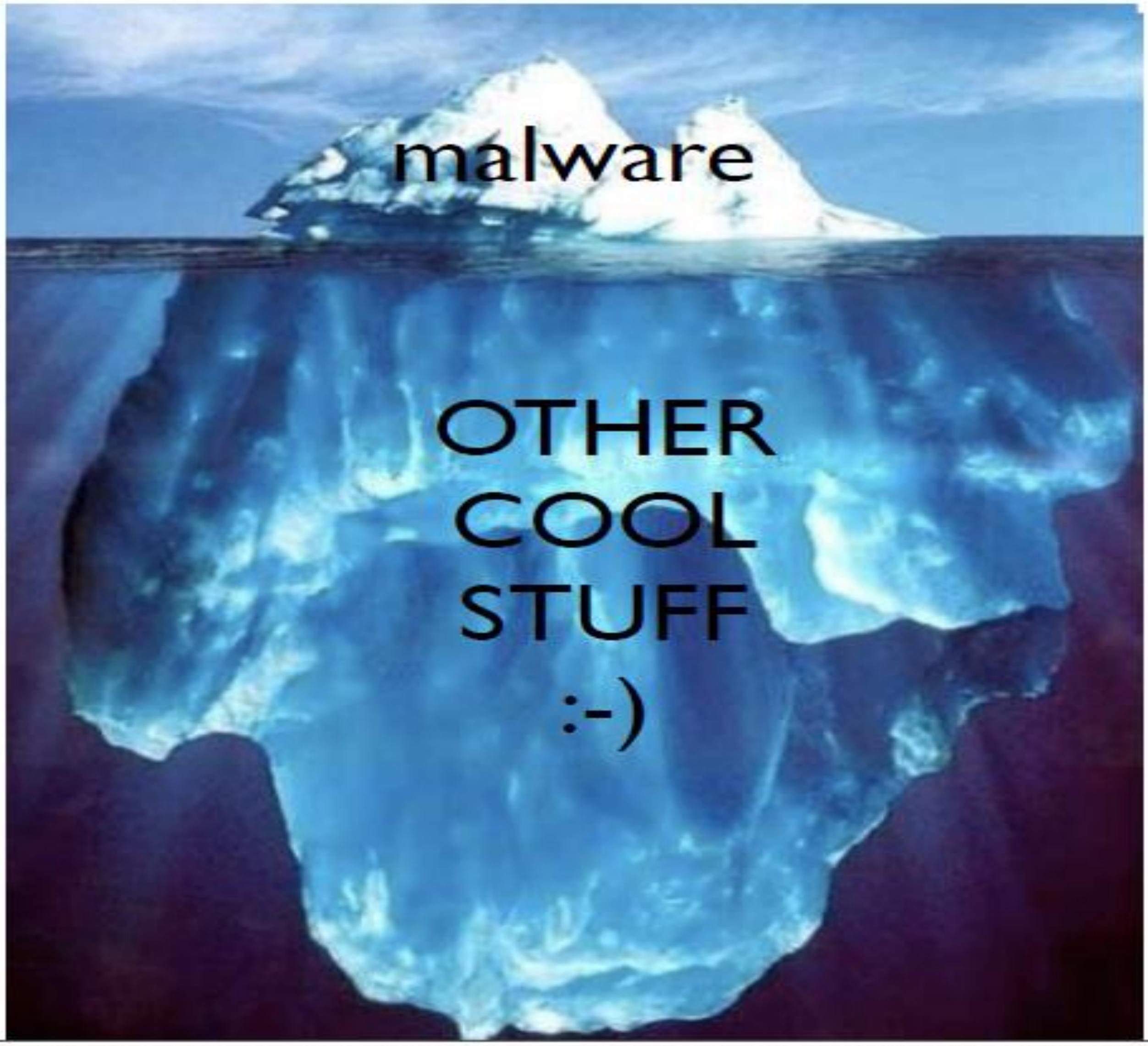
Who are the hackers?

Why such spike?

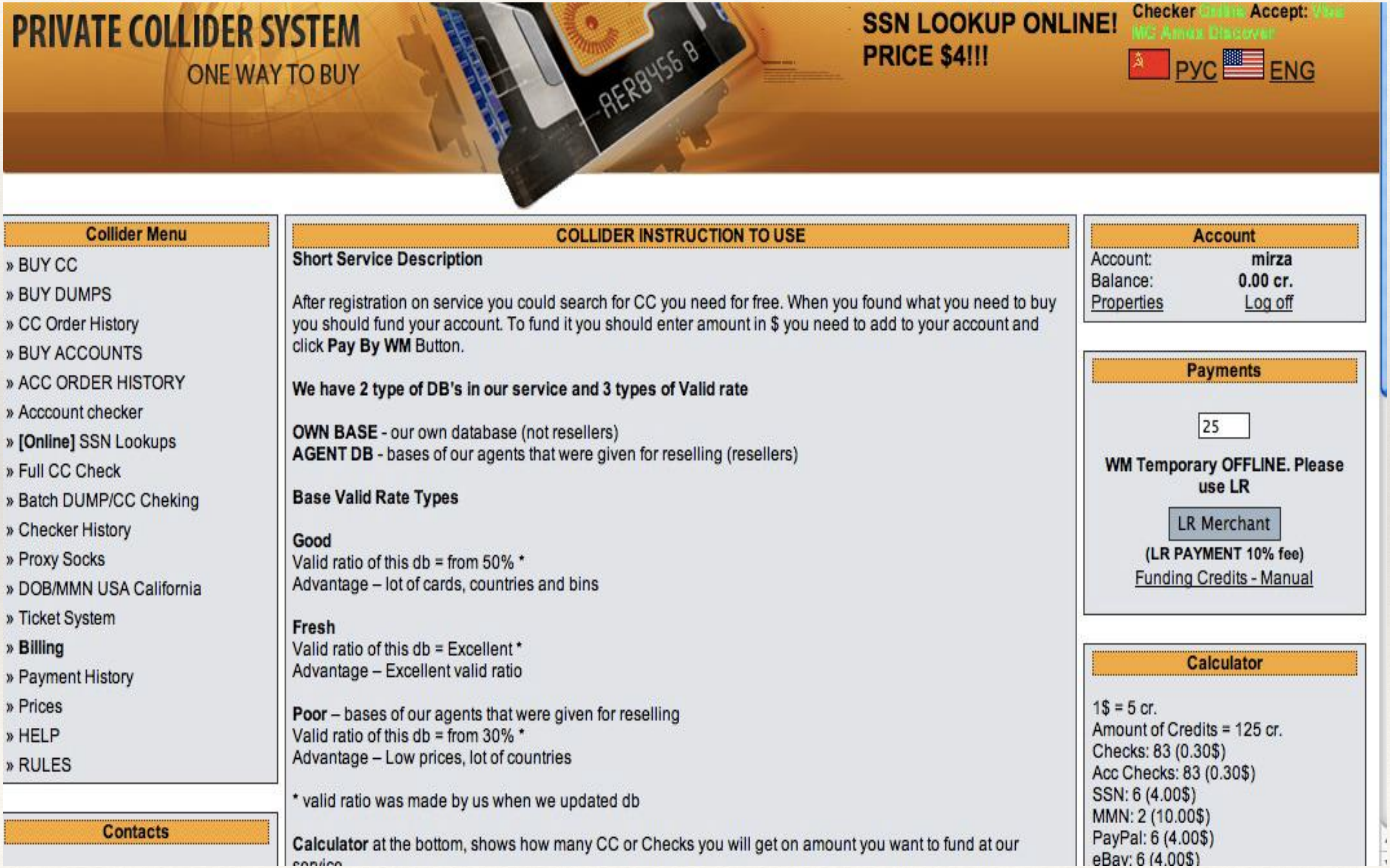
- Fun?
- Profit!

Who are the hackers?

But there's much more..



Who are the hackers?



PRIVATE COLLIDER SYSTEM

ONE WAY TO BUY

SSN LOOKUP ONLINE!
PRICE $4!!!

Checker Online Accept: Visa MC Amex Discover

РУС ENG

Collider Menu

- » BUY CC
- » BUY DUMPS
- » CC Order History
- » BUY ACCOUNTS
- » ACC ORDER HISTORY
- » Acccount checker
- » **[Online]** SSN Lookups
- » Full CC Check
- » Batch DUMP/CC Cheking
- » Checker History
- » Proxy Socks
- » DOB/MMN USA California
- » Ticket System
- » **Billing**
- » Payment History
- » Prices
- » HELP
- » RULES

Contacts

COLLIDER INSTRUCTION TO USE

Short Service Description

After registration on service you could search for CC you need for free. When you found what you need to buy you should fund your account. To fund it you should enter amount in $ you need to add to your account and click **Pay By WM** Button.

We have 2 type of DB's in our service and 3 types of Valid rate

OWN BASE - our own database (not resellers)
AGENT DB - bases of our agents that were given for reselling (resellers)

Base Valid Rate Types

Good
Valid ratio of this db = from 50% *
Advantage – lot of cards, countries and bins

Fresh
Valid ratio of this db = Excellent *
Advantage – Excellent valid ratio

Poor – bases of our agents that were given for reselling
Valid ratio of this db = from 30% *
Advantage – Low prices, lot of countries

* valid ratio was made by us when we updated db

Calculator at the bottom, shows how many CC or Checks you will get on amount you want to fund at our service

Account

Account:	**mirza**
Balance:	**0.00 cr.**
Properties	Log off

Payments

25

WM Temporary OFFLINE. Please use LR

LR Merchant

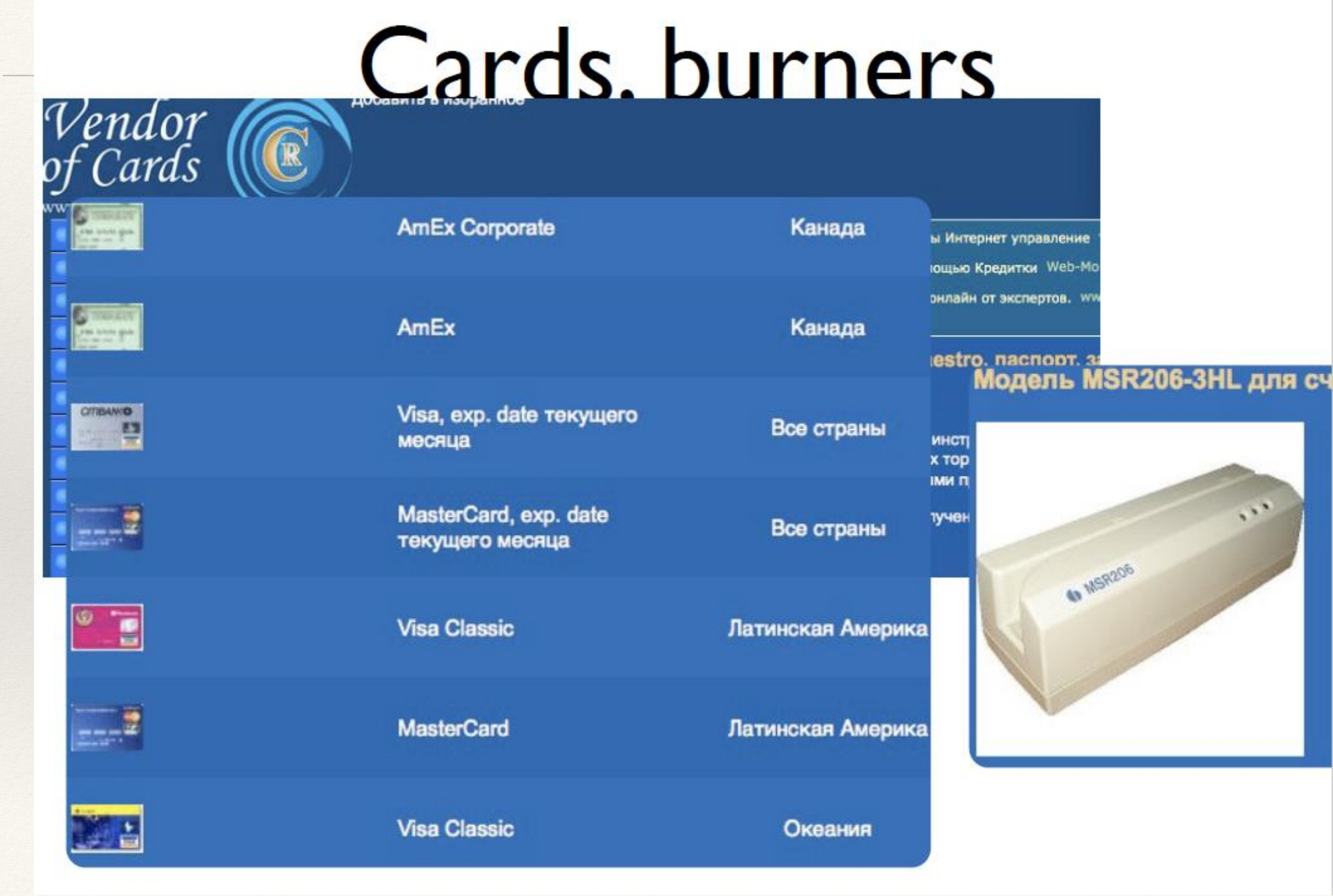
(LR PAYMENT 10% fee)

Funding Credits - Manual

Calculator

1$ = 5 cr.
Amount of Credits = 125 cr.
Checks: 83 (0.30$)
Acc Checks: 83 (0.30$)
SSN: 6 (4.00$)
MMN: 2 (10.00$)
PayPal: 6 (4.00$)
eBay: 6 (4.00$)

Who are the hackers?



Cards, burners

Добавить в избранное

Vendor of Cards

	AmEx Corporate	Канада
	AmEx	Канада
	Visa, exp. date текущего месяца	Все страны
	MasterCard, exp. date текущего месяца	Все страны
	Visa Classic	Латинская Америка
	MasterCard	Латинская Америка
	Visa Classic	Океания

ы Интернет управление

ощью Кредитки Web-Mo

онлайн от экспертов. ww

estro, паспорт, з

инстр

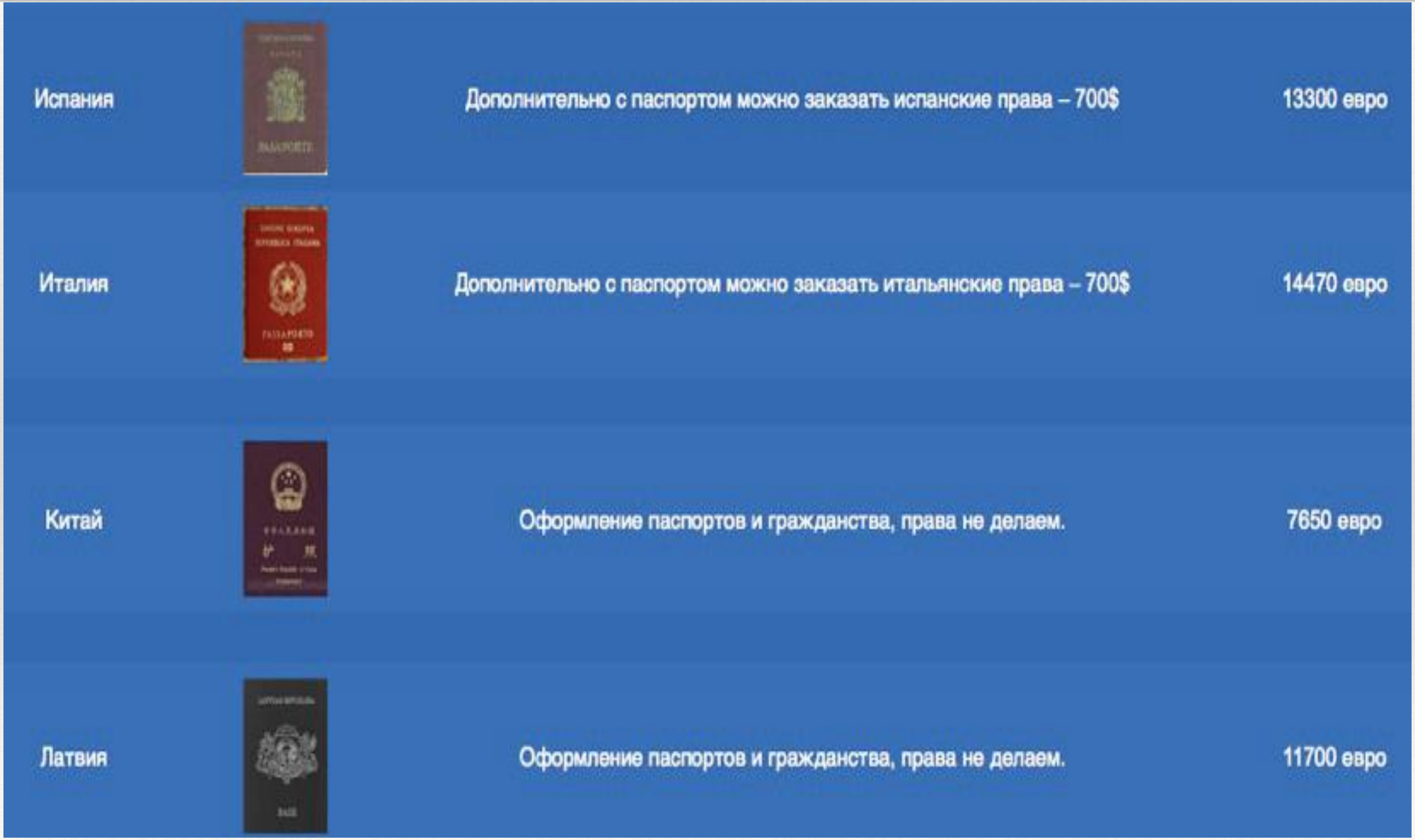
х тор

ими п

лучен

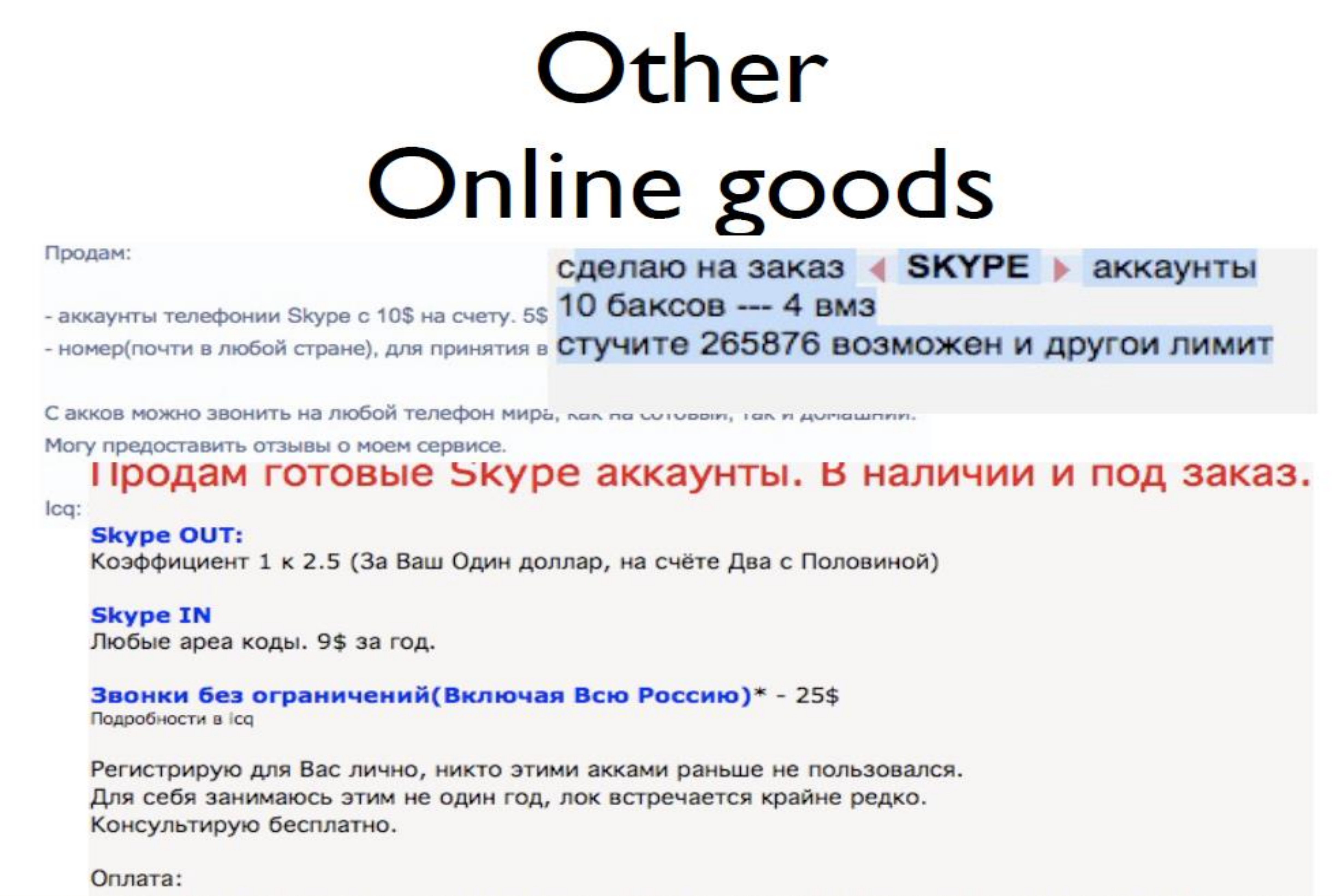
Модель MSR206-3HL для сч

Who are the hackers?



Испания		Дополнительно с паспортом можно заказать испанские права – 700$	13300 евро
Италия		Дополнительно с паспортом можно заказать итальянские права – 700$	14470 евро
Китай		Оформление паспортов и гражданства, права не делаем.	7650 евро
Латвия		Оформление паспортов и гражданства, права не делаем.	11700 евро

Who are the hackers?



Other Online goods

Продам:

- аккаунты телефонии Skype с 10$ на счету. 5$
- номер(почти в любой стране), для принятия в

С акков можно звонить на любой телефон мира, как на сотовый, так и домашний.

Могу предоставить отзывы о моем сервисе.

Icq:

сделаю на заказ ◂ SKYPE ▸ аккаунты
10 баксов --- 4 вмз
стучите 265876 возможен и другои лимит

Продам готовые Skype аккаунты. В наличии и под заказ.

Skype OUT:
Коэффициент 1 к 2.5 (За Ваш Один доллар, на счёте Два с Половиной)

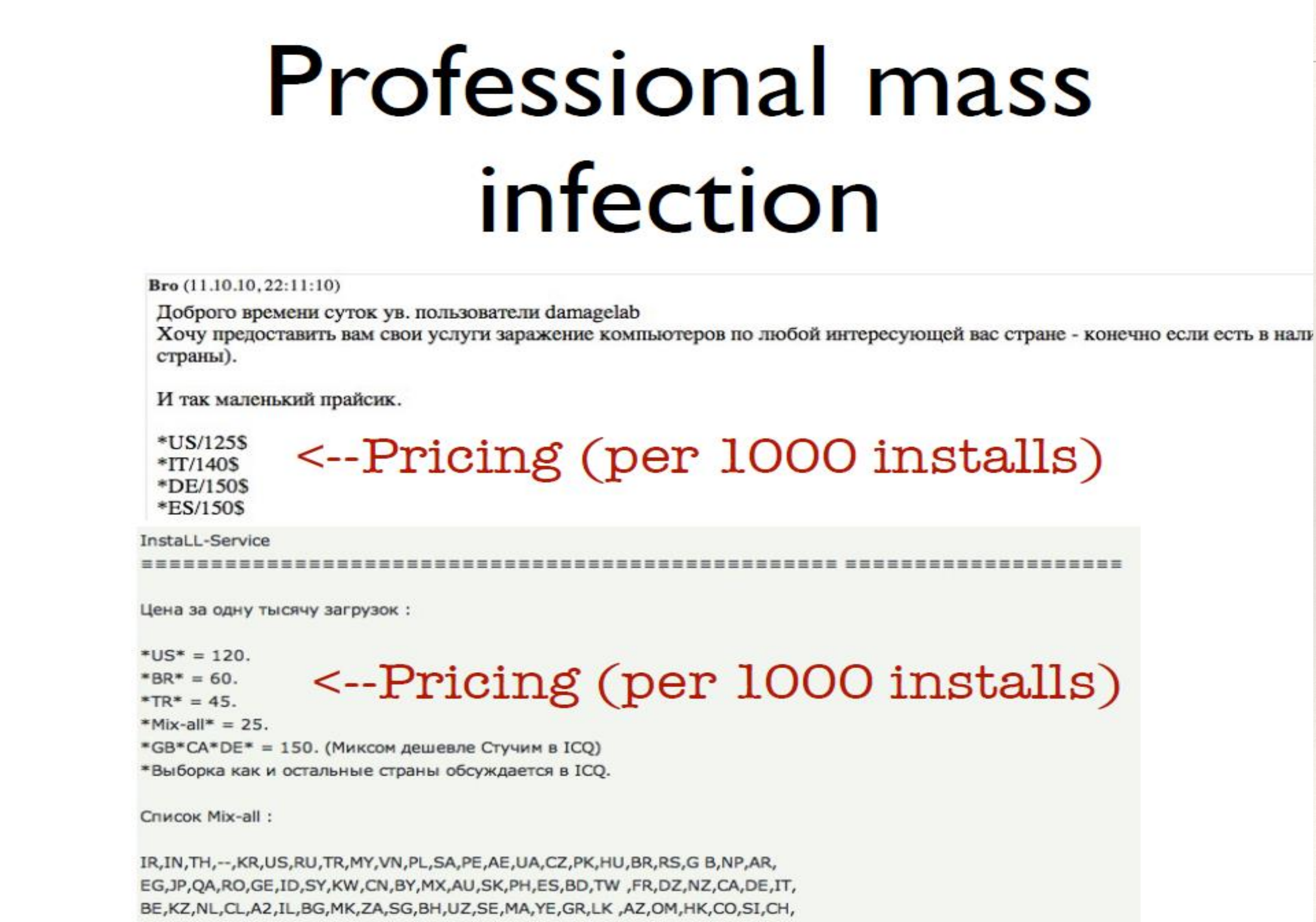
Skype IN
Любые ареа коды. 9$ за год.

Звонки без ограничений(Включая Всю Россию)* - 25$
Подробности в icq

Регистрирую для Вас лично, никто этими акками раньше не пользовался.
Для себя занимаюсь этим не один год, лок встречается крайне редко.
Консультирую бесплатно.

Оплата:

Who are the hackers?



Professional mass infection

Bro (11.10.10, 22:11:10)

Доброго времени суток ув. пользователи damagelab
Хочу предоставить вам свои услуги заражение компьютеров по любой интересующей вас стране - конечно если есть в нали
страны).

И так маленький прайсик.

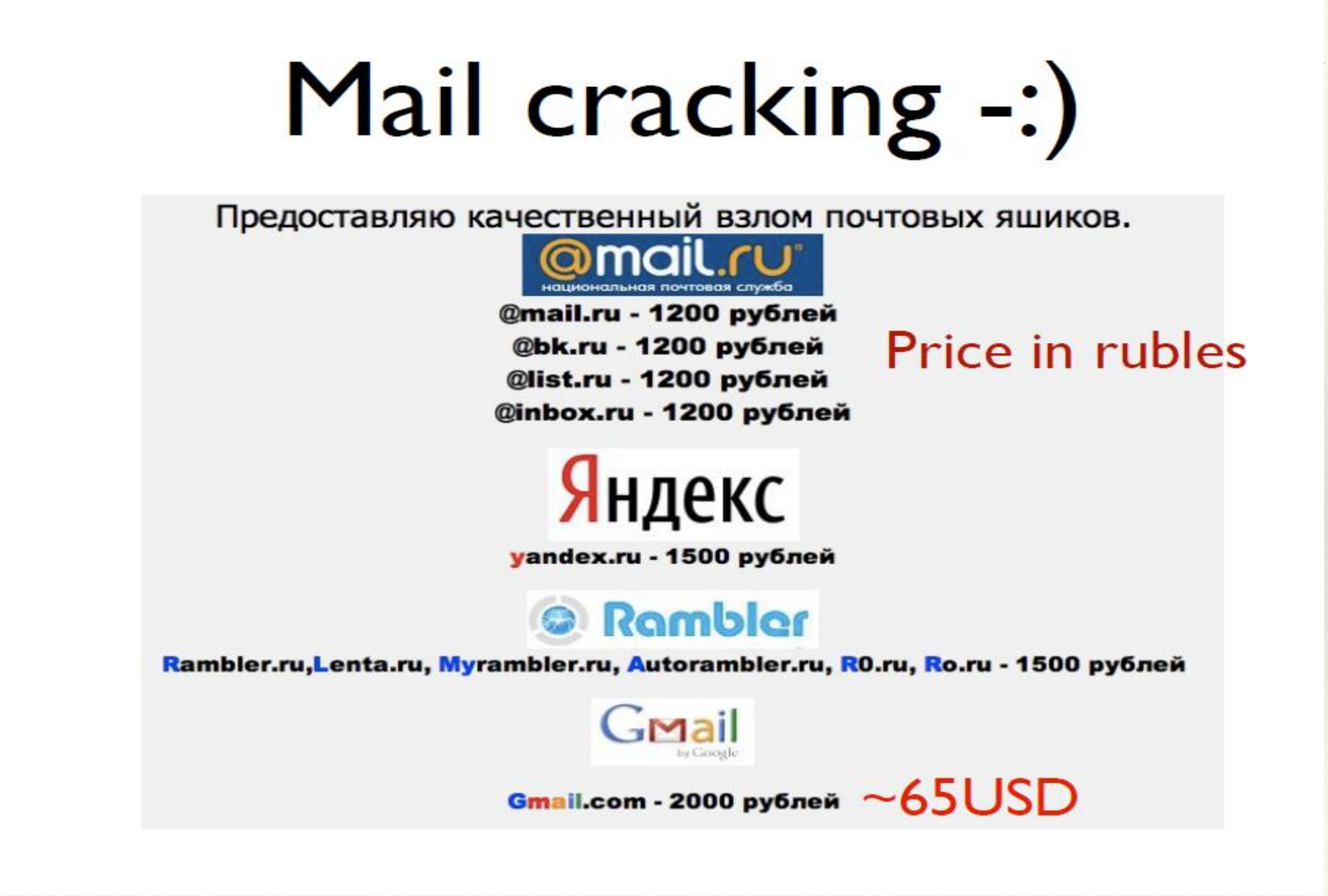
*US/125$
*IT/140$
*DE/150$
*ES/150$

<--Pricing (per 1000 installs)

```
InstaLL-Service
============================================================ ======================

Цена за одну тысячу загрузок :

*US* = 120.
*BR* = 60.
*TR* = 45.
*Mix-all* = 25.
*GB*CA*DE* = 150. (Миксом дешевле Стучим в ICQ)
*Выборка как и остальные страны обсуждается в ICQ.

Список Mix-all :

IR,IN,TH,--,KR,US,RU,TR,MY,VN,PL,SA,PE,AE,UA,CZ,PK,HU,BR,RS,G B,NP,AR,
EG,JP,QA,RO,GE,ID,SY,KW,CN,BY,MX,AU,SK,PH,ES,BD,TW ,FR,DZ,NZ,CA,DE,IT,
BE,KZ,NL,CL,A2,IL,BG,MK,ZA,SG,BH,UZ,SE,MA,YE,GR,LK ,AZ,OM,HK,CO,SI,CH,
```

<--Pricing (per 1000 installs)

Who are the hackers?



@mail.ru
национальная почтовая служба
Яндекс
Rambler
Gmail
by Google

Mail cracking -:)

Предоставляю качественный взлом почтовых яшиков.

@mail.ru - 1200 рублей
@bk.ru - 1200 рублей
@list.ru - 1200 рублей
@inbox.ru - 1200 рублей

Price in rubles

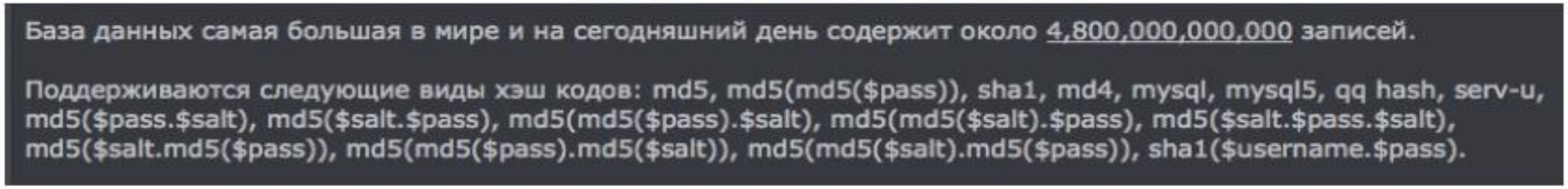
yandex.ru - 1500 рублей

Rambler.ru,Lenta.ru, Myrambler.ru, Autorambler.ru, R0.ru, Ro.ru - 1500 рублей

Gmail.com - 2000 рублей ~65USD

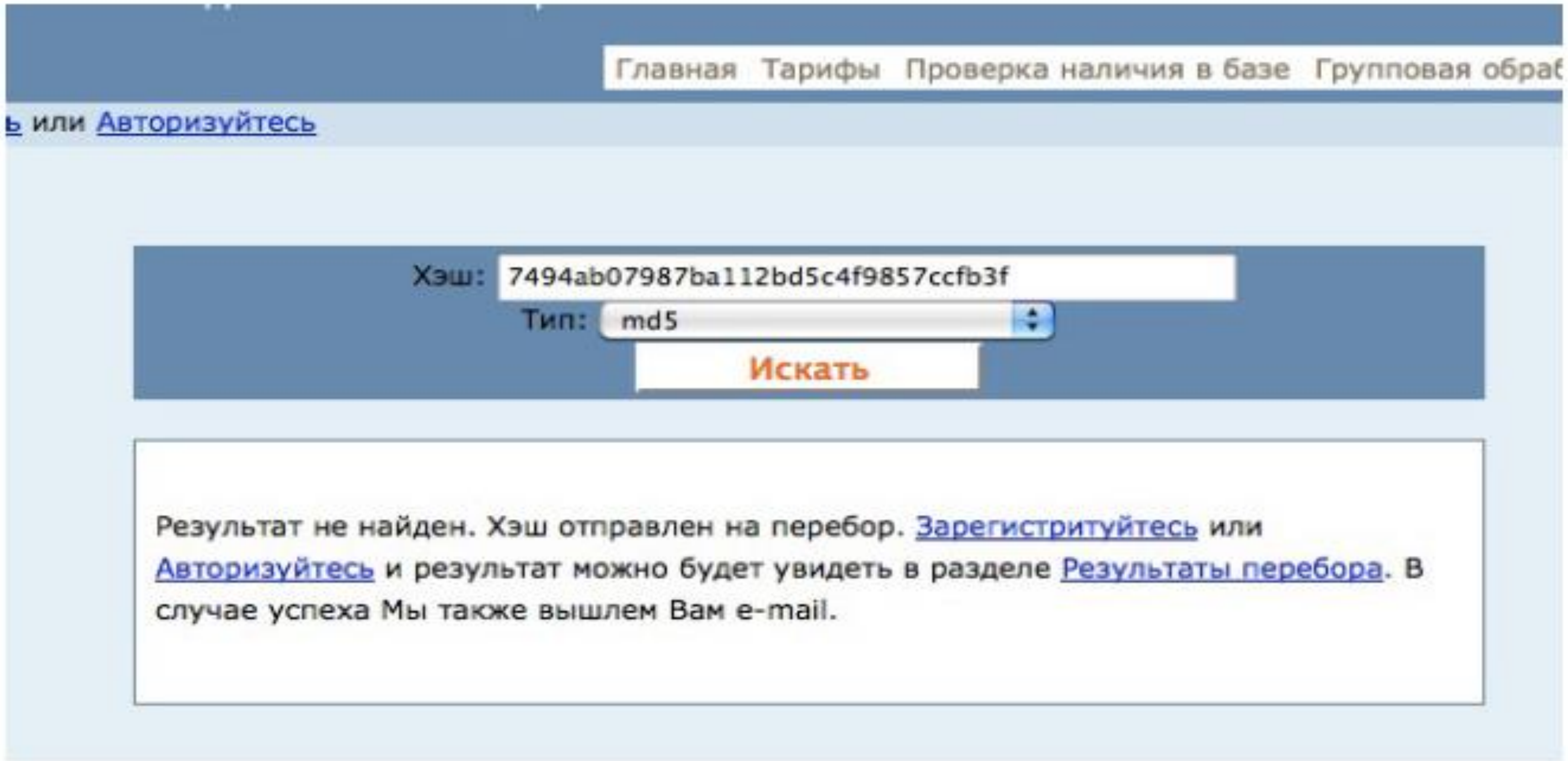
Who are the hackers?

Hash cracking
In cloud



База данных самая большая в мире и на сегодняшний день содержит около 4,800,000,000,000 записей.

Поддерживаются следующие виды хэш кодов: md5, md5(md5($pass)), sha1, md4, mysql, mysql5, qq hash, serv-u, md5($pass.$salt), md5($salt.$pass), md5(md5($pass).$salt), md5(md5($salt).$pass), md5($salt.$pass.$salt), md5($salt.md5($pass)), md5(md5($pass).md5($salt)), md5(md5($salt).md5($pass)), sha1($username.$pass).



Хэш: 7494ab07987ba112bd5c4f9857ccfb3f

Тип: md5

Результат не найден. Хэш отправлен на перебор. Зарегистрируйтесь или Авторизуйтесь и результат можно будет увидеть в разделе Результаты перебора. В случае успеха Мы также вышлем Вам e-mail.

Who are the hackers?

Saw the news? :)

WANTED

BY THE FBI

FBI's Operation ACHing Mule

FEDERAL CYBER CRIME CHARGES

Ilya Karasev

Dmitry Saprunov

Lilian Adam

Marina Oprea

Are we bad guys?

Saw the news? :)

WANTED
BY THE FBI

FBI's Operation ACHing Mule

FEDERAL CYBER CRIME CHARGES

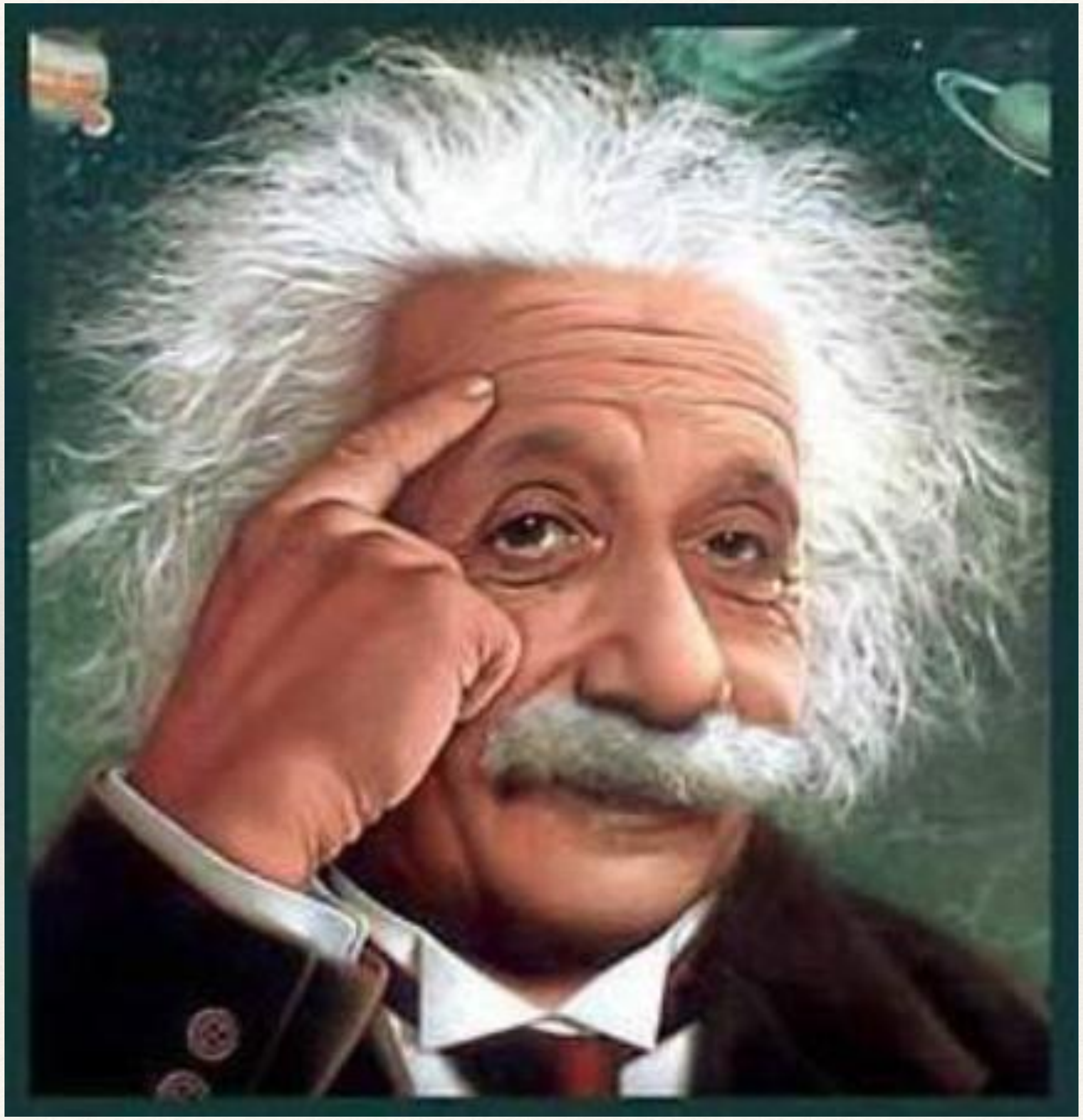
Ilya Karasev

Dmitry Saprunov

Lilian Adam

Marina Oprea

Why standards?



Standards

- Standards are basic recommendations that are very flexible and can be easily adapted.
- Many organizations are afraid to adapt a standard as they think that they are hard or complex and would require them to change their business processes. However, standards do not require companies to change their processes. Standards do not recommend physical technology or methods as a solution.
- We will show some standard techniques to demonstrate how it can be implemented in your day-to-day operations.

Frameworks

- anything written
- PCI?
- HITRUST??
- Cloud Security Alliance???

PCI Security Standards Council ®

HITRUST CSF Certified

CSA cloud security alliance ®

Standards

- ISO
- NIST
- SSAE 18?

Standards

Cyber Security standards are industry accepted principals with objectives to reduce risks and prevent or mitigate cyber attacks.

Most accepted standards in USA:

ISO 27001

Pros:

- International
- Certifiable
- Widely recognized and accepted

Cons:

- Procedural
- Top-down – executives have to buy in

NIST

Pros:

- US national standard
- US laws are based on NIST
- Can be adapted on a department level

Cons:

- Not certifiable – self attestation

PCI

Pros:

- Very active standard enforced by banks
- Certifiable

Cons:

- E-commerce specific
- Not recognized in financial and manufacturing world

SOC

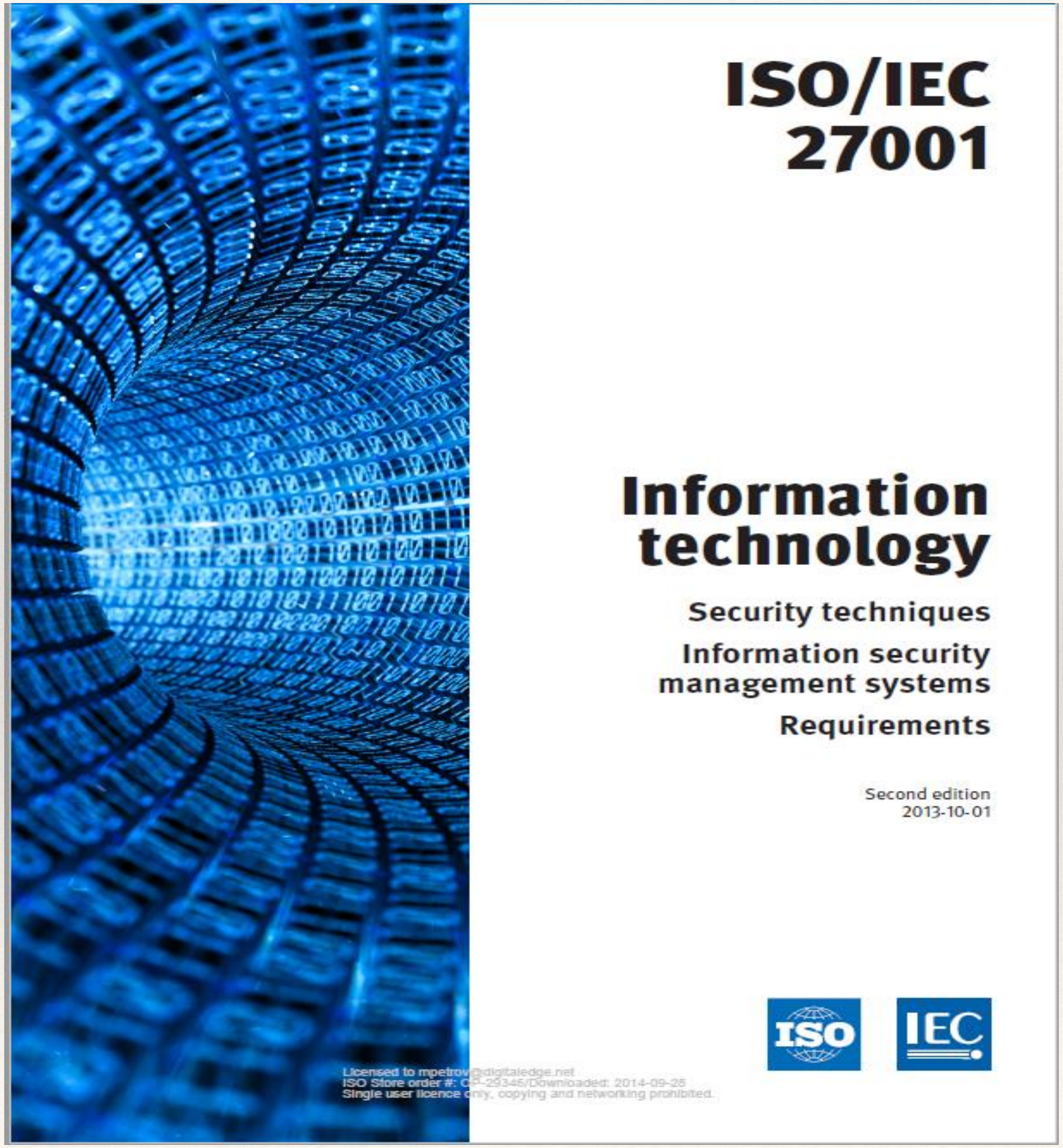
Pros:

- Concentrates on overall stability of the company, not just security controls.
- Certifiable

Cons:

- A loose report sometimes demonstrating an opinion
- The report is often not in-depth

They look boring



ISO/IEC
27001

Information
technology

Security techniques

Information security
management systems

Requirements

Second edition
2013-10-01

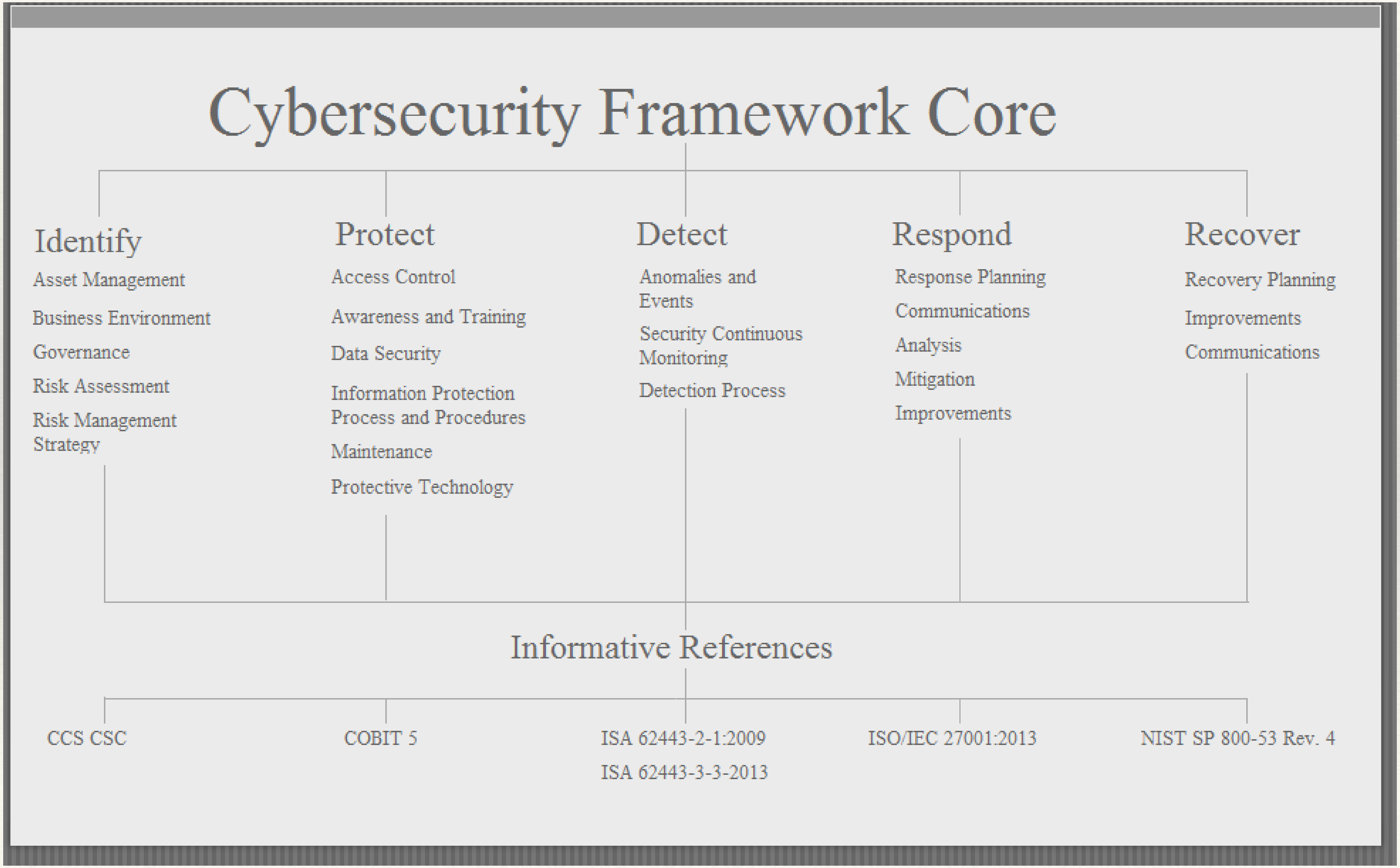
ISO structure

1. Context of the organization
2. Leadership
3. Planning
4. Support
5. Operation
6. Performance Evaluation
7. Improvement
8. Annex (Controls)

ISO structure - Annex

1. Information Security Policies
2. Organization of Information Security
3. Human Resources Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communication Security
10. System Acquisition, Development Maintenance
11. Supplier Relationship
12. Information Security Incident Management
13. Compliance

NIST structure



Cybersecurity Framework Core

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Information Protection Process and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications

Informative References

- CCS CSC
- COBIT 5
- ISA 62443-2-1:2009
- ISA 62443-3-3-2013
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 4

SSAE 18 SOC2

- SECURITY PRINCIPLE:

❑ ORGANIZATION AND MANAGEMENT
❑ COMMUNICATIONS
❑ RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS
❑ MONITORING OF CONTROLS
❑ LOGICAL AND PHYSICAL ACCESS CONTROLS
❑ LOGICAL AND PHYSICAL ACCESS
❑ SYSTEM OPERATIONS
❑ CHANGE MANAGEMENT

- THE AVAILABILITY PRINCIPLE:

❑ ADDITIONAL CRITERIA

- PROCESSING INTEGRITY:

❑ ADDITIONAL CRITERIA

- CONFIDENTIALITY:

❑ ADDITIONAL CRITERIA

- PRIVACY:

❑ ADDITIONAL CRITERIA

Day 1 take away

1. All standards are mostly the same
2. They look hard but when you understand the structure they are not complex
3. You need to know the difference to make the right selection
4. They are all good

Exercise

1. What is your first action if you are noticed or notified about a security incident?

❑ Eradicate intruder
❑ Check policies and procedures
❑ Preserve artifacts for future forensic

2. Write a case for an appropriate framework for your organization.
3. What do you do if you are breached, possibly 10,000 PIIs disclosed, and you have users in NY and Alabama

Rate the day

❑ 5. Learned good amount
❑ 4. Learned some
❑ 3. Learned a bit
❑ 2. Learned nothing
❑ 1. Didn’t listen/didn’t care

Day 2

Standards vs Hackers and Lawmakers

Michael Petrov
CEO

Digital Edge

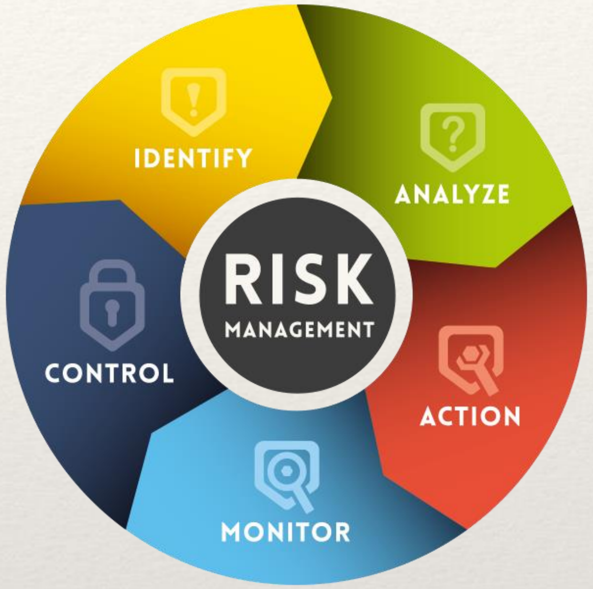
ISACA
Trust in, and value from, information systems

Agenda – Day 2

- Risks – general facts
- 2 Ways of thinking about risk
- Risk -> Controls / Controls -> Risk
- Common approach
- Implementation spiral
- Discussion/examples

It is all about 2 things

Private
CONFIDENTIAL
Sensitive
PUBLIC

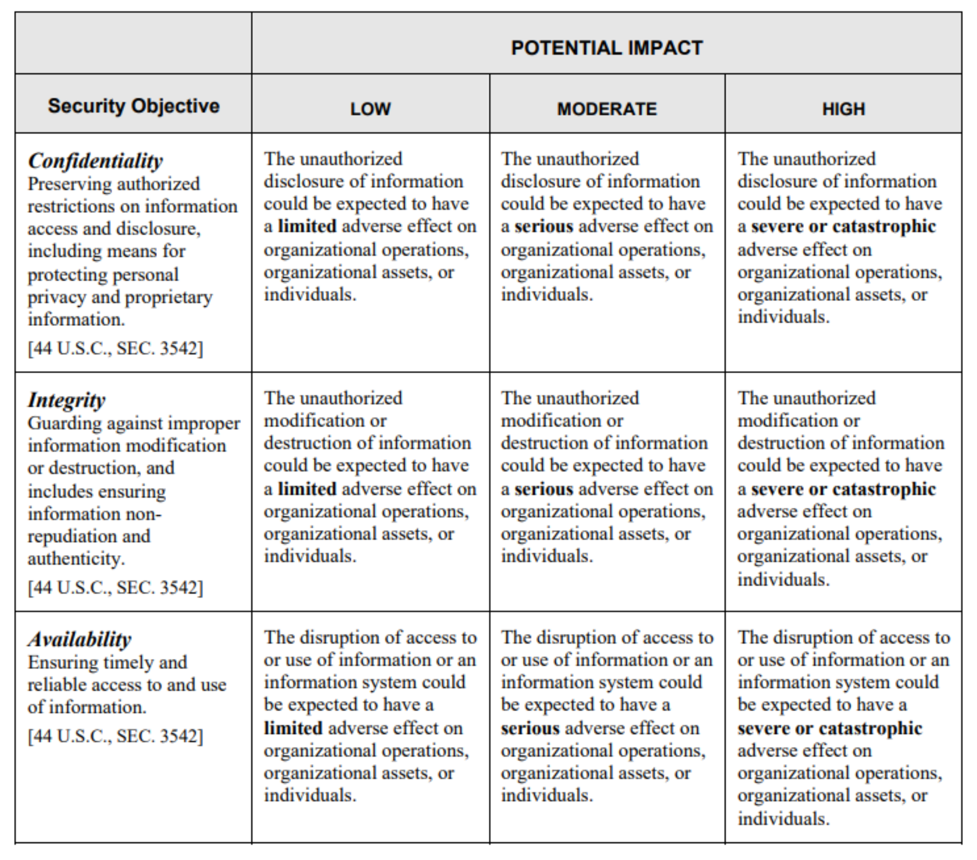


CONTEXT

Information Classification

FIPS
https://csrc.nist.gov/publications/detail/fips/199/final

CIA factor



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Risk

Problems with SCRM

- It is very important
- No standardization

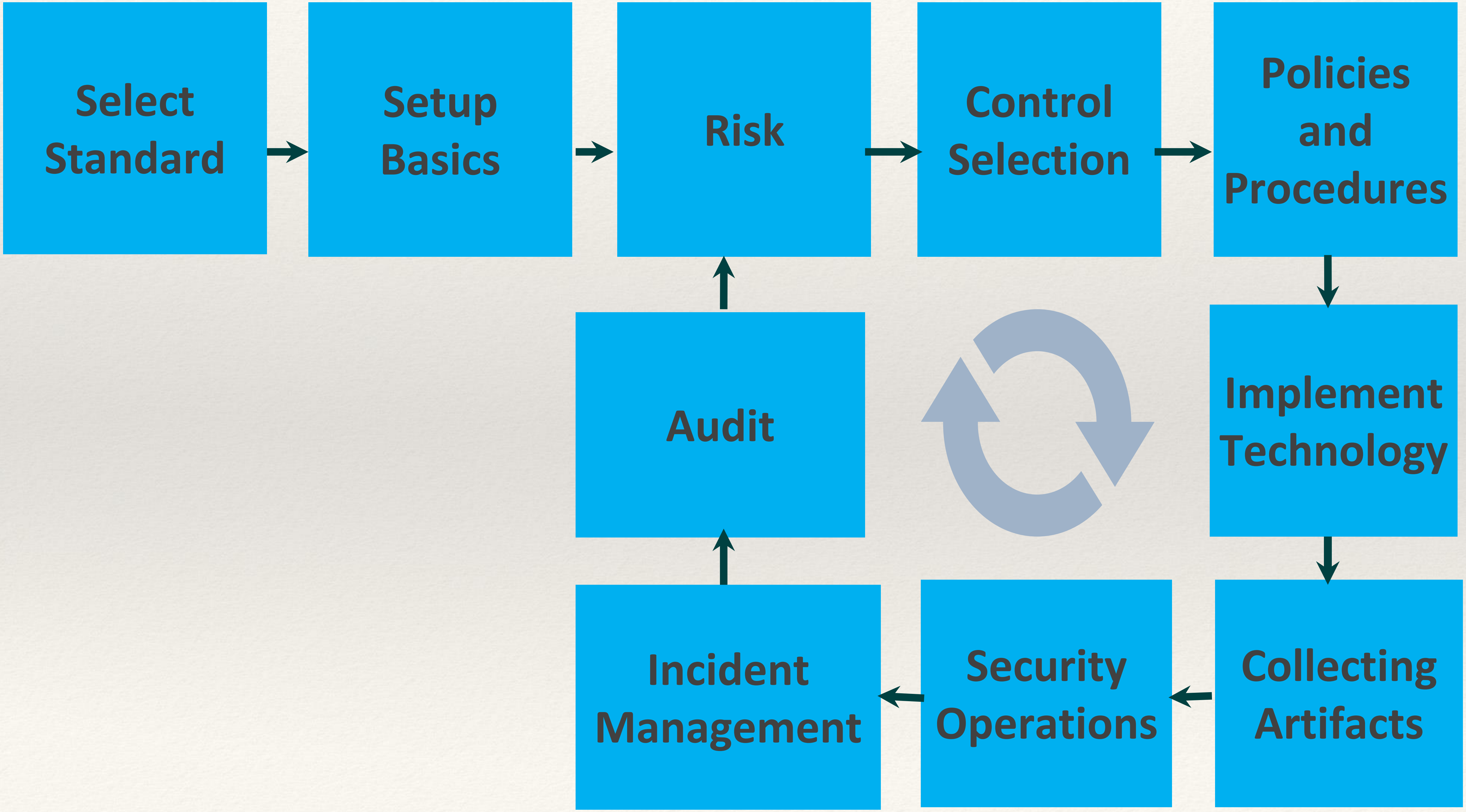
“Decisions are often made based on individual’s instinct and knowledge of conventional wisdom and typical practices” – NIST.IR 8286

- System based approach problems
- Likelihood ⇔ Impact ⇔ Rating
- FAIR

https://www.fairinstitute.org/about

- Risk appetite. “Email service shall be available during large majority of a 24 hour period.
- Risk tolerance: “Email service shall not be interrupted more then 5 minutes during core hours”

Simplifying standards



Select Standard

Setup Basics

Risk

Control Selection

Policies and Procedures

Implement Technology

Collecting Artifacts

Security Operations

Incident Management

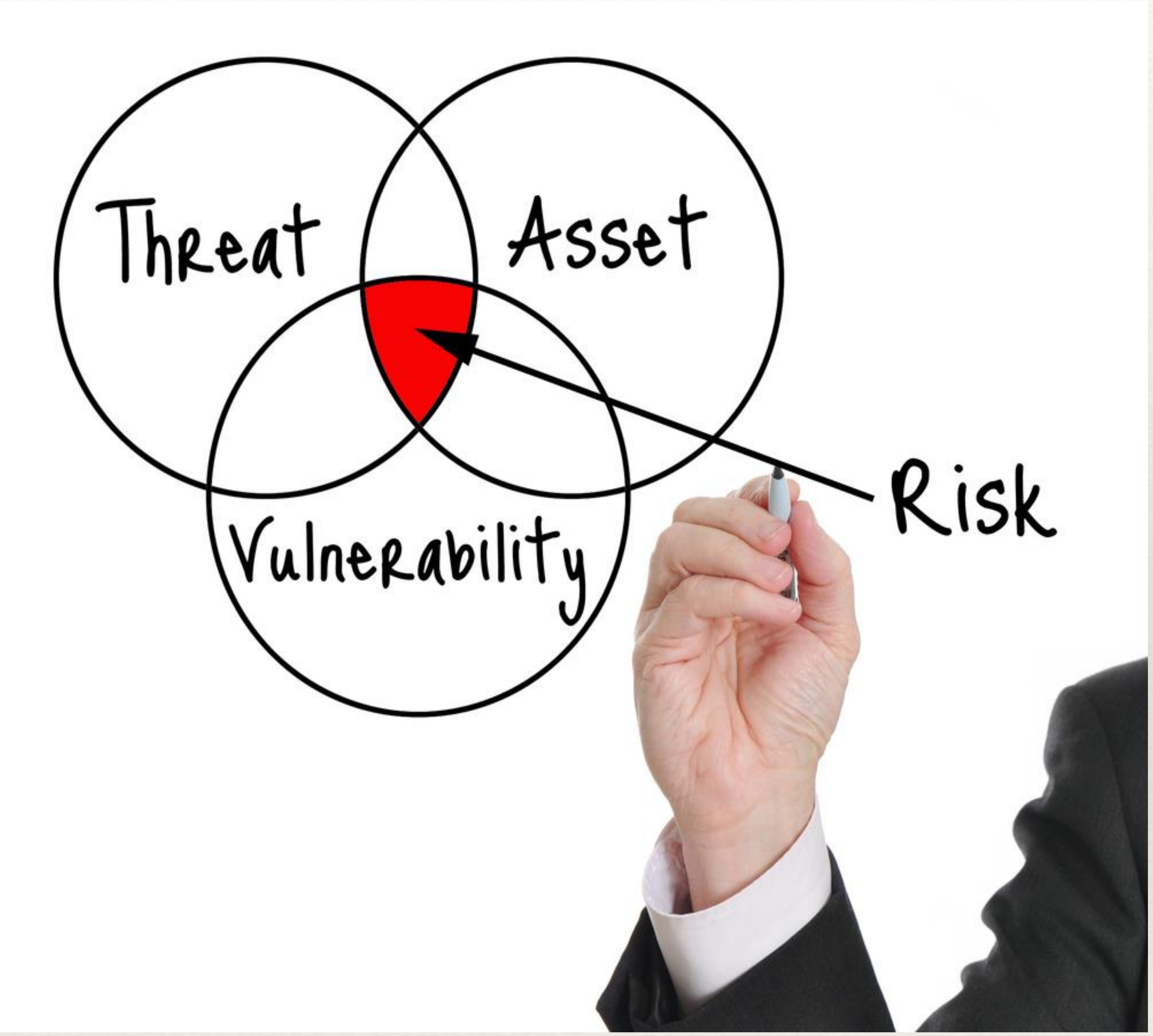
Audit

SETUP BASICS

- Governance
- Information and system classification
- Required laws and compliance
- Scope

RISKS

- Identification
- Classification
- Management
- Policies and procedures



CONTROL SELECTION

- Select applicable controls from the standard
- Review sufficiency
- Applicability statement

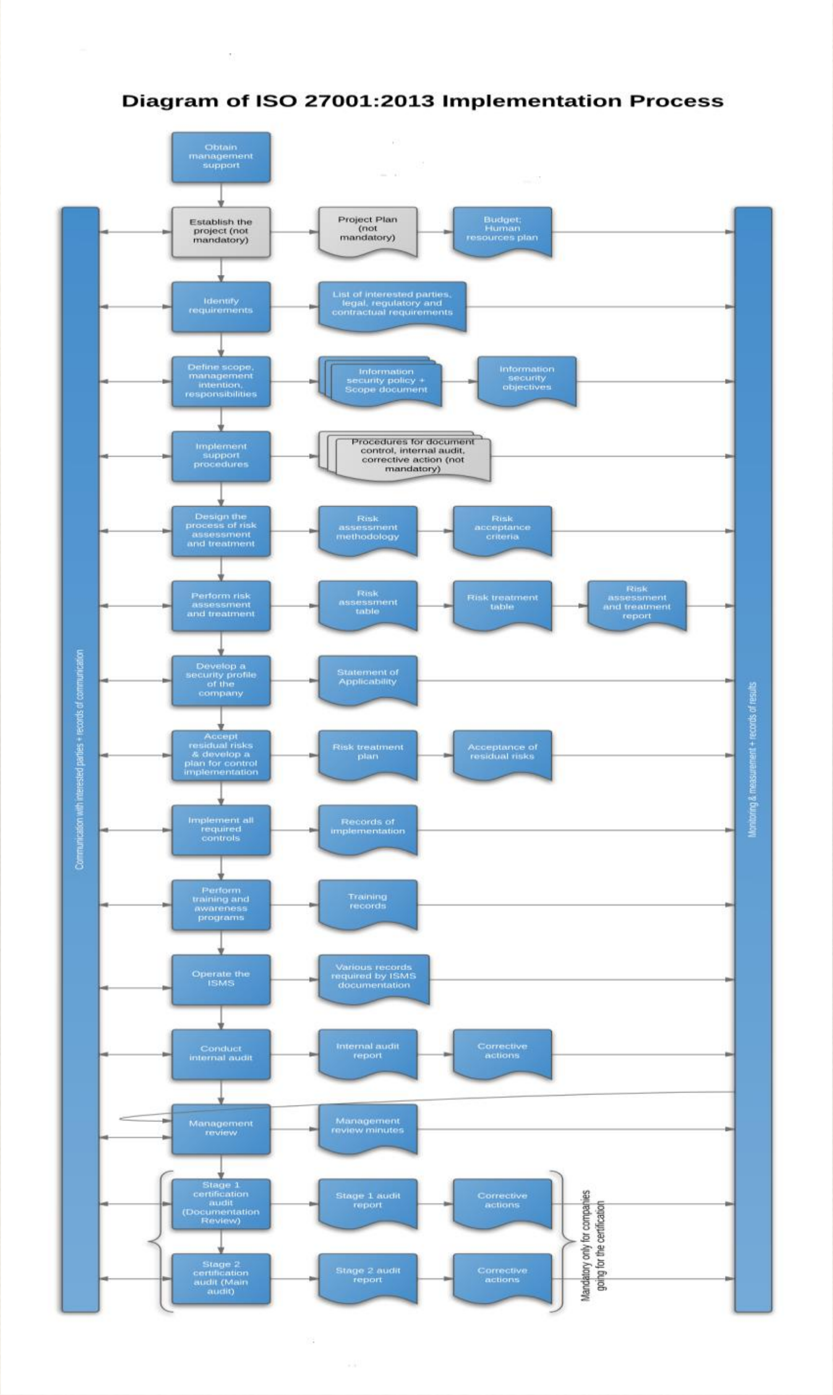


Diagram of ISO 27001:2013 Implementation Process
Obtain management support
Establish the project (not mandatory)
Project Plan (not mandatory)
Budget; Human resources plan
Identify requirements
List of interested parties, legal, regulatory and contractual requirements
Define scope, management intention, responsibilities
Information security policy + Scope document
Information security objectives
Implement support procedures
Procedures for document control, internal audit, corrective action (not mandatory)
Design the process of risk assessment and treatment
Risk assessment methodology
Risk acceptance criteria
Perform risk assessment and treatment
Risk assessment table
Risk treatment table
Risk assessment and treatment report
Develop a security profile of the company
Statement of Applicability
Accept residual risks & develop a plan for control implementation
Risk treatment plan
Acceptance of residual risks
Implement all required controls
Records of implementation
Perform training and awareness programs
Training records
Operate the ISMS
Various records required by ISMS documentation
Conduct internal audit
Internal audit report
Corrective actions
Management review
Management review minutes
Stage 1 certification audit (Documentation Review)
Stage 1 audit report
Corrective actions
Stage 2 certification audit (Main audit)
Stage 2 audit report
Corrective actions
Mandatory only for companies going for the certification
Communication with interested parties + records of communication
Monitoring & measurement + records of results

POLICIES AND PROCEDURES

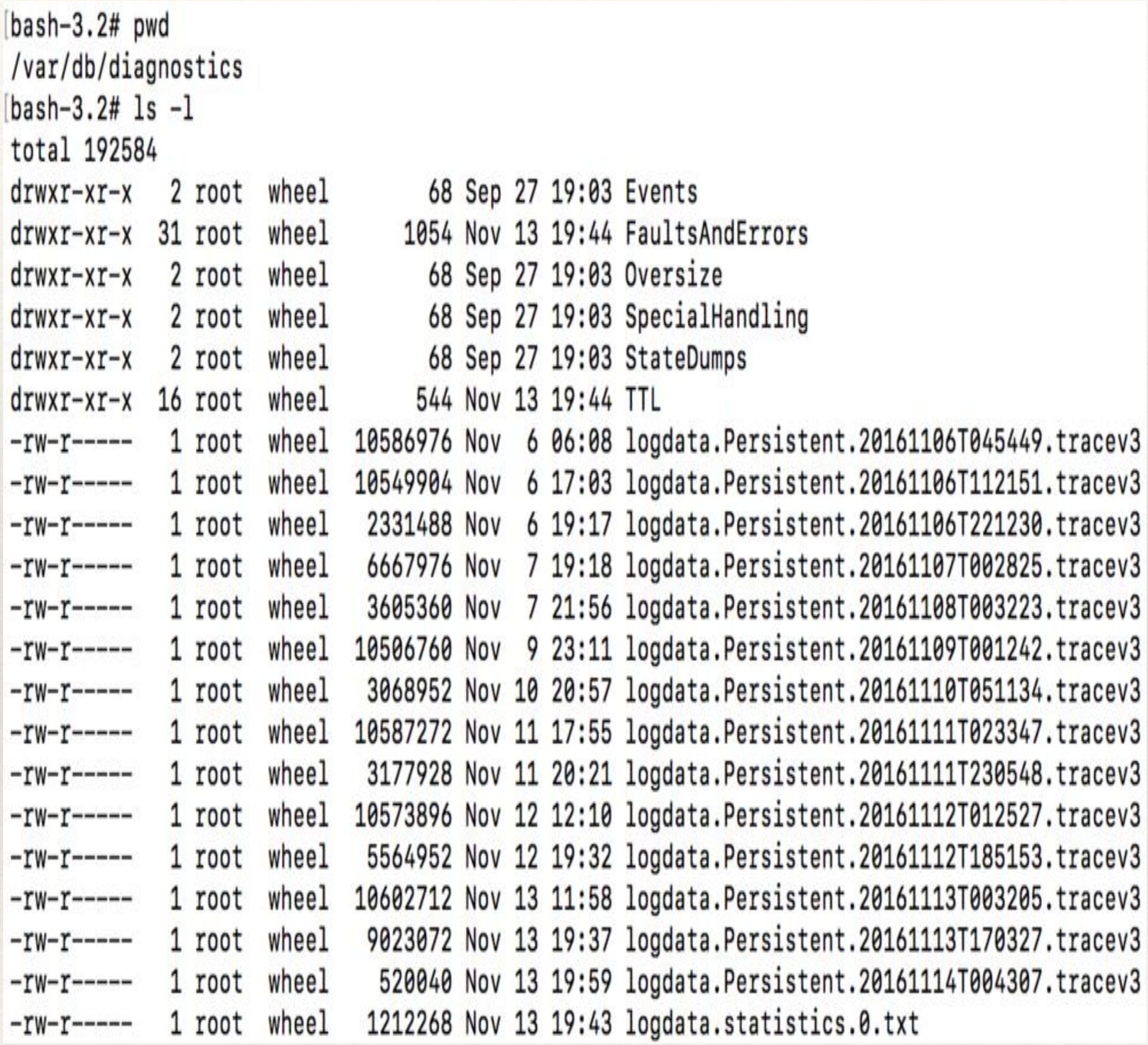
- Documentation
- Awareness
- Management approval

TECHNOLOGY IMPLEMENTATION

- Review controls and required artifacts
- Additional implementations and compensations
- Monitoring and review

COLLECT ARTIFACTS

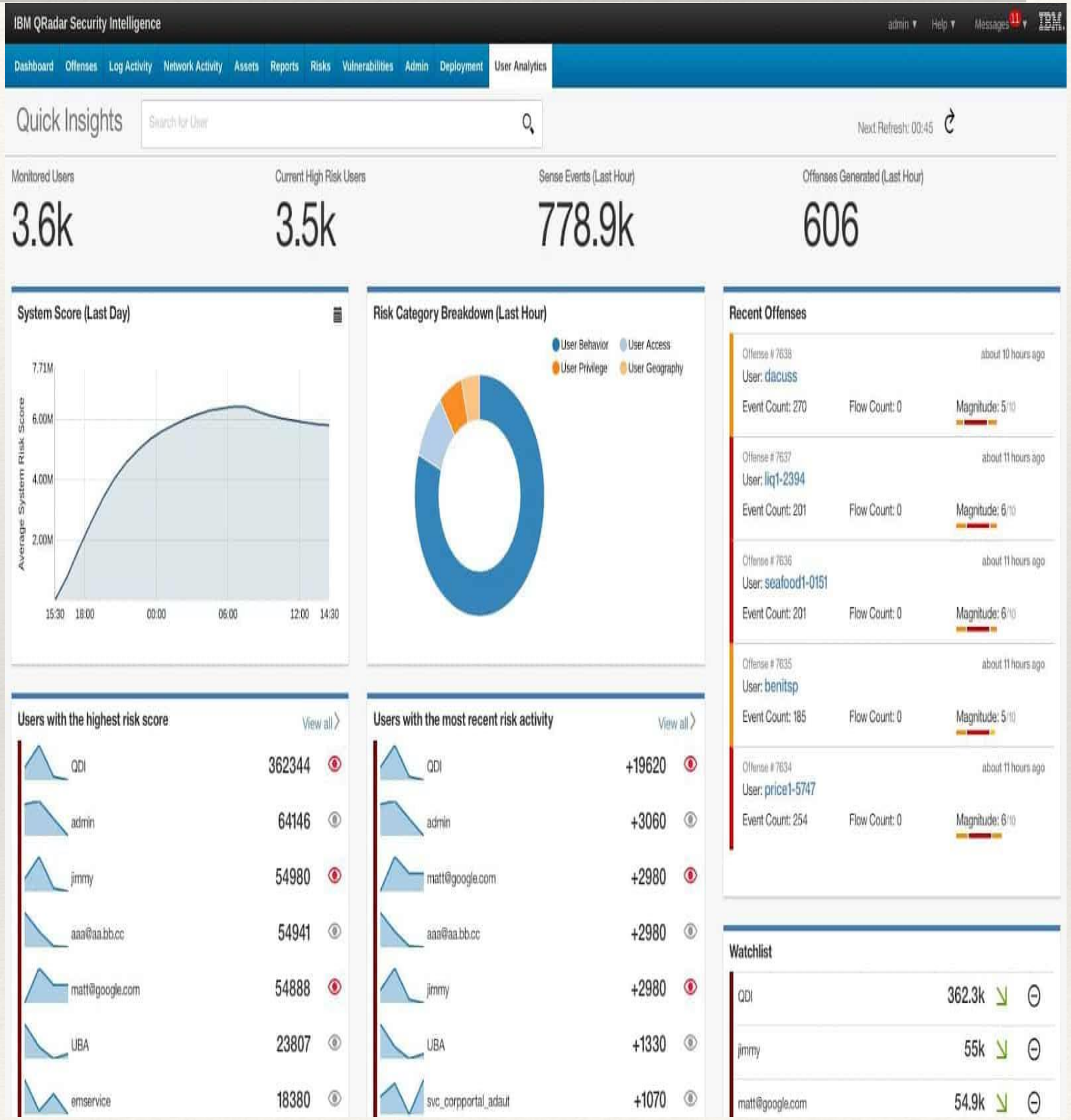
- Review controls and required artifacts
- Additional implementations and compensations
- Monitoring and review



```
bash-3.2# pwd
/var/db/diagnostics
bash-3.2# ls -l
total 192584
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 Events
drwxr-xr-x  31 root  wheel     1054 Nov 13 19:44 FaultsAndErrors
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 Oversize
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 SpecialHandling
drwxr-xr-x   2 root  wheel       68 Sep 27 19:03 StateDumps
drwxr-xr-x  16 root  wheel      544 Nov 13 19:44 TTL
-rw-r-----   1 root  wheel 10586976 Nov  6 06:08 logdata.Persistent.20161106T045449.tracev3
-rw-r-----   1 root  wheel 10549904 Nov  6 17:03 logdata.Persistent.20161106T112151.tracev3
-rw-r-----   1 root  wheel  2331488 Nov  6 19:17 logdata.Persistent.20161106T221230.tracev3
-rw-r-----   1 root  wheel  6667976 Nov  7 19:18 logdata.Persistent.20161107T002825.tracev3
-rw-r-----   1 root  wheel  3605360 Nov  7 21:56 logdata.Persistent.20161108T003223.tracev3
-rw-r-----   1 root  wheel 10506760 Nov  9 23:11 logdata.Persistent.20161109T001242.tracev3
-rw-r-----   1 root  wheel  3068952 Nov 10 20:57 logdata.Persistent.20161110T051134.tracev3
-rw-r-----   1 root  wheel 10587272 Nov 11 17:55 logdata.Persistent.20161111T023347.tracev3
-rw-r-----   1 root  wheel  3177928 Nov 11 20:21 logdata.Persistent.20161111T230548.tracev3
-rw-r-----   1 root  wheel 10573896 Nov 12 12:10 logdata.Persistent.20161112T012527.tracev3
-rw-r-----   1 root  wheel  5564952 Nov 12 19:32 logdata.Persistent.20161112T185153.tracev3
-rw-r-----   1 root  wheel 10602712 Nov 13 11:58 logdata.Persistent.20161113T003205.tracev3
-rw-r-----   1 root  wheel  9023072 Nov 13 19:37 logdata.Persistent.20161113T170327.tracev3
-rw-r-----   1 root  wheel   520040 Nov 13 19:59 logdata.Persistent.20161114T004307.tracev3
-rw-r-----   1 root  wheel  1212268 Nov 13 19:43 logdata.statistics.0.txt
```

SECURITY OPERATIONS

- Security Information and Event Management
- Reviews and SOPs
- Escalations



Quick Insights

Monitored Users	Current High Risk Users	Sense Events (Last Hour)	Offenses Generated (Last Hour)
3.6k	3.5k	778.9k	606

Users with the highest risk score

QDI	362344
admin	64146
jimmy	54980
aaa@aa.bb.cc	54941
matt@google.com	54888
UBA	23807
emservice	18380

Users with the most recent risk activity

QDI	+19620
admin	+3060
matt@google.com	+2980
aaa@aa.bb.cc	+2980
jimmy	+2980
UBA	+1330
svc_corpportal_adaut	+1070

Recent Offenses

Offense	Time	User	Event Count	Flow Count	Magnitude
Offense # 7638	about 10 hours ago	dacuss	270	0	5/10
Offense # 7637	about 11 hours ago	liq1-2394	201	0	6/10
Offense # 7636	about 11 hours ago	seafood1-0151	201	0	6/10
Offense # 7635	about 11 hours ago	benitsp	185	0	5/10
Offense # 7634	about 11 hours ago	price1-5747	254	0	6/10

Watchlist

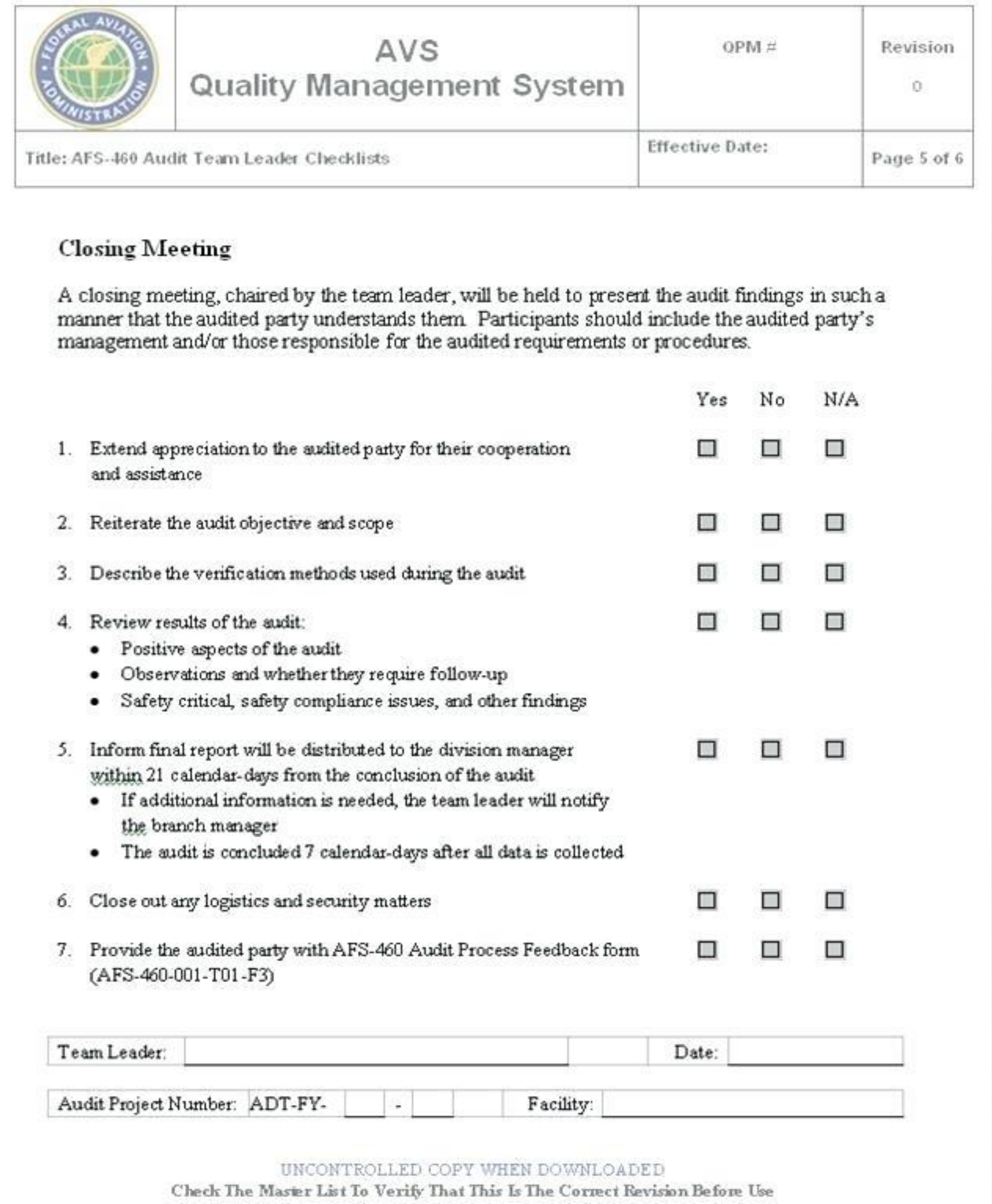
QDI	362.3k ↘
jimmy	55k ↘
matt@google.com	54.9k ↘

INCIDENT MANAGEMENT

- CIRT operations
- Notification
- Documentation
- Risk correlation and measurements

INTERNAL AUDIT

- Checkboxes vs self continues Due Diligence process
- Scheduled reviews
- Internal Audits
- Management reviews



	AVS Quality Management System	OPM #	Revision 0
Title: AFS-460 Audit Team Leader Checklists		Effective Date:	Page 5 of 6

Closing Meeting

A closing meeting, chaired by the team leader, will be held to present the audit findings in such a manner that the audited party understands them. Participants should include the audited party's management and/or those responsible for the audited requirements or procedures.

	Yes	No	N/A
1. Extend appreciation to the audited party for their cooperation and assistance	□	□	□
2. Reiterate the audit objective and scope	□	□	□
3. Describe the verification methods used during the audit	□	□	□
4. Review results of the audit: • Positive aspects of the audit • Observations and whether they require follow-up • Safety critical, safety compliance issues, and other findings	□	□	□
5. Inform final report will be distributed to the division manager within 21 calendar-days from the conclusion of the audit • If additional information is needed, the team leader will notify the branch manager • The audit is concluded 7 calendar-days after all data is collected	□	□	□
6. Close out any logistics and security matters	□	□	□
7. Provide the audited party with AFS-460 Audit Process Feedback form (AFS-460-001-T01-F3)	□	□	□

Team Leader: ______________________ Date: ____________

Audit Project Number: ADT-FY- ____ - ____ Facility: ______________________

UNCONTROLLED COPY WHEN DOWNLOADED
Check The Master List To Verify That This Is The Correct Revision Before Use

OUR ATTITUDE

Select Standard → Setup Basics → Risk → Control Selection → Policies and Procedures → Implement Technology → Collecting Artifacts → Security Operations → Incident Management → Audit → Risk

Day 2 takeaway

- It is easy when it is structured
- It is easy to jump between standards
- It is not static, must be alive
- It is cyclical

Rate the day

- ❑ 5. Learned good amount
- ❑ 4. Learned some
- ❑ 3. Learned a bit
- ❑ 2. Learned nothing
- ❑ 1. Didn’t listen/didn’t care

Exercise

- Create an excel file for information classification
- Create an excel file for risk registry
- Create an excel file for incident registry

Day 3

Standards vs Hackers and Lawmakers

Michael Petrov
CEO

Digital Edge

ISACA®
Trust in, and value from, information systems

Agenda – Day 3

- Zero Trust
- Practical Examples/Suggestions
  - Information Classification
  - Risks
  - Incidents
  - Control maturity (forgot to mention)
  - Policies and Procedures
  - KPIs
  - Education management
  - Reviews and Audits
  - BCP
  - Laws and regulations
- Specificities of frameworks
- Privacy
- Funny bouts

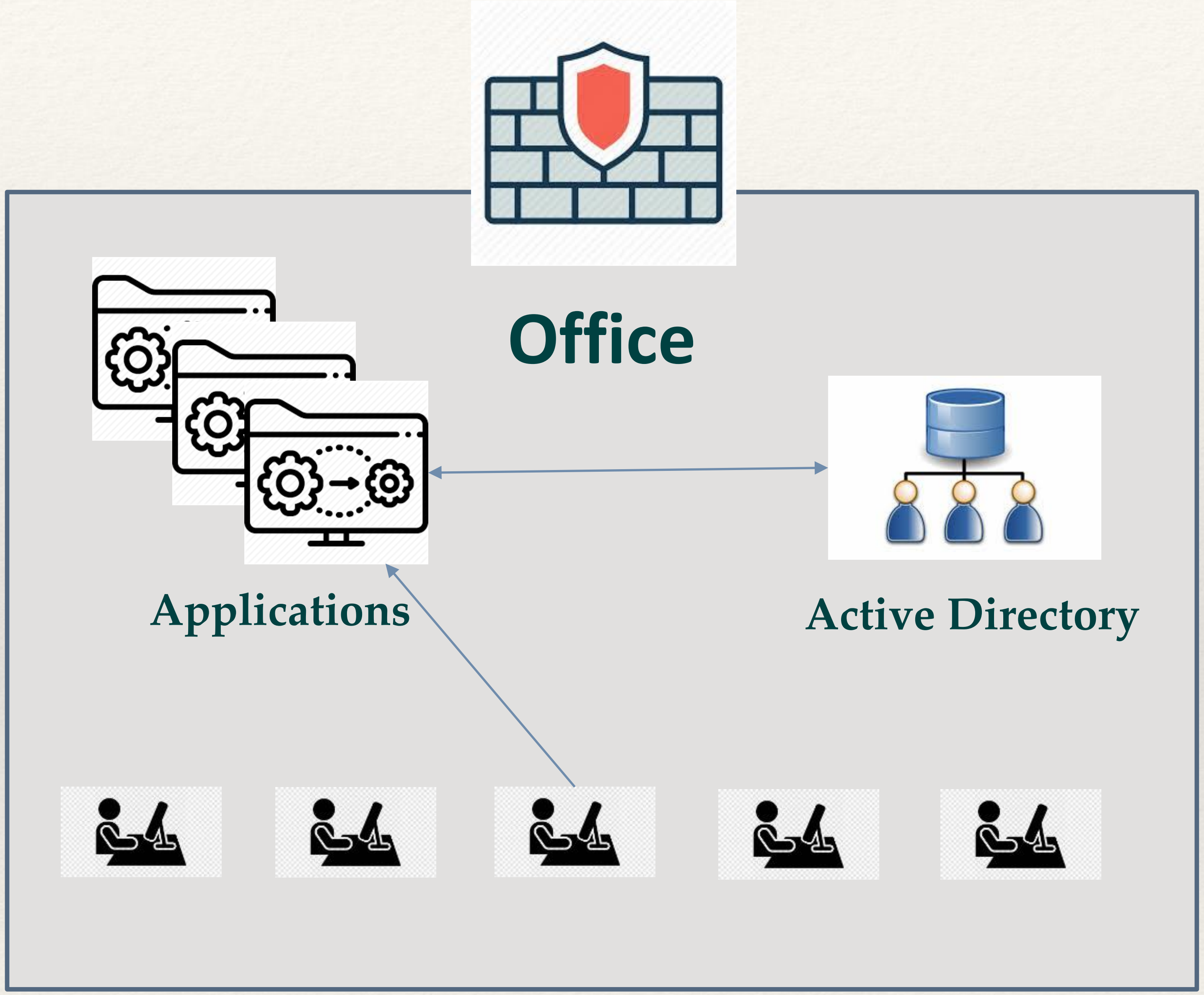
Zero Trust (requested by Vince Werling)

https://www.youtube.com/watch?v=tFrbt9s4Fns

Paul Simmonds – HISTERICAL

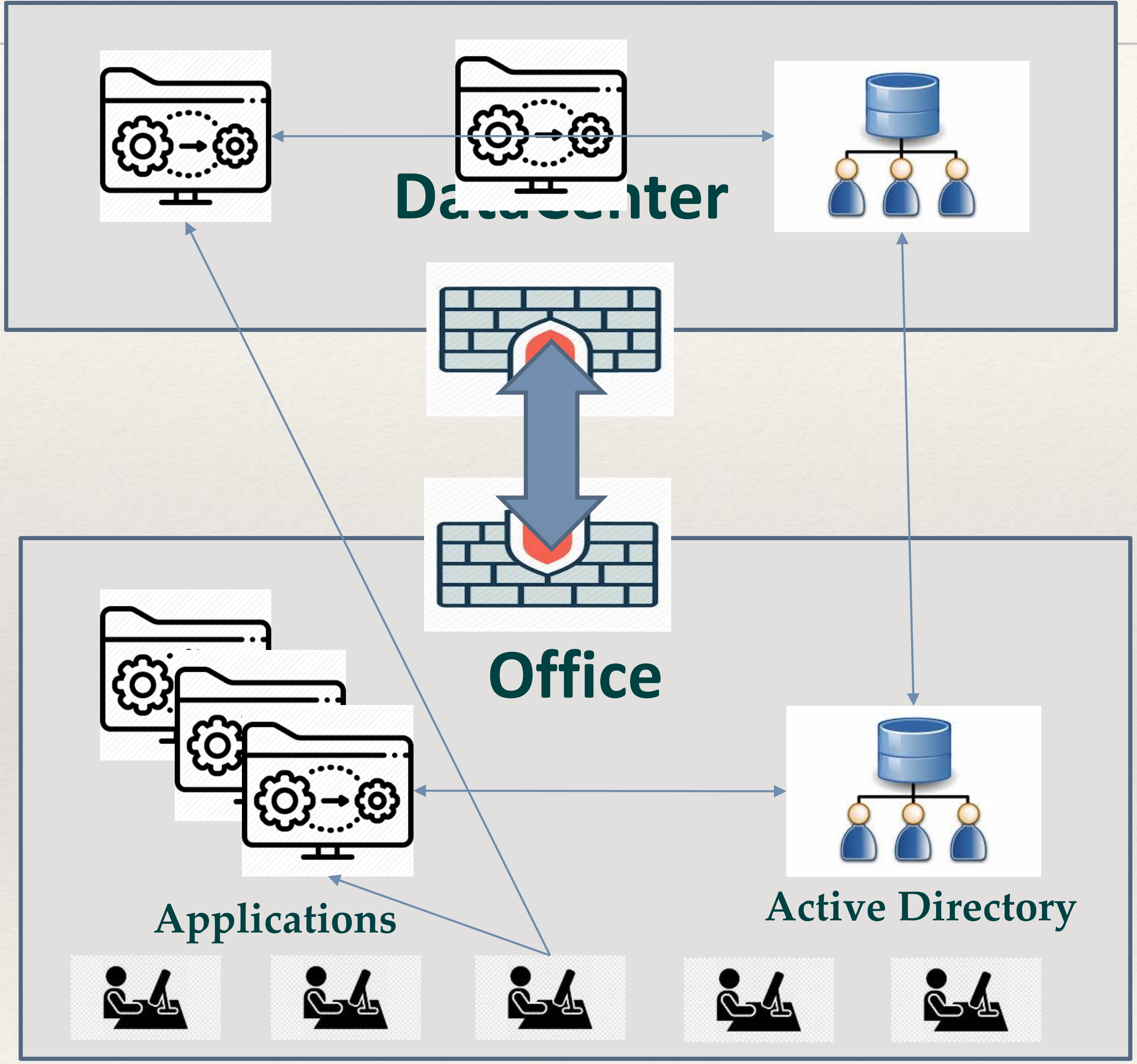
…ACCESS MANAGEMENT IS REALLY KEY…

Standard, perimeter-based security



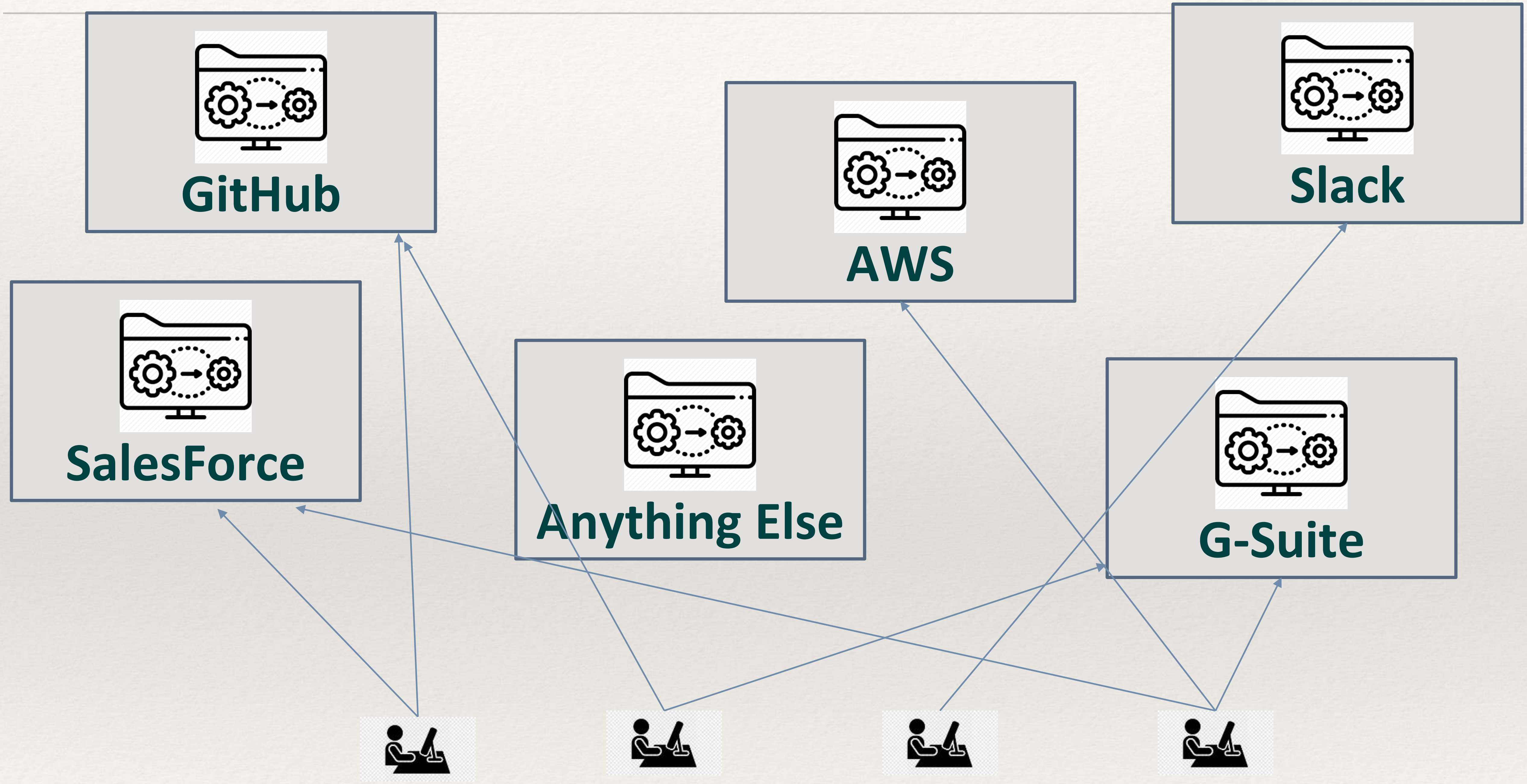
Cybersecurity will always challenge you.
But we will give you the **EDGE**.

Standard, perimeter-based security



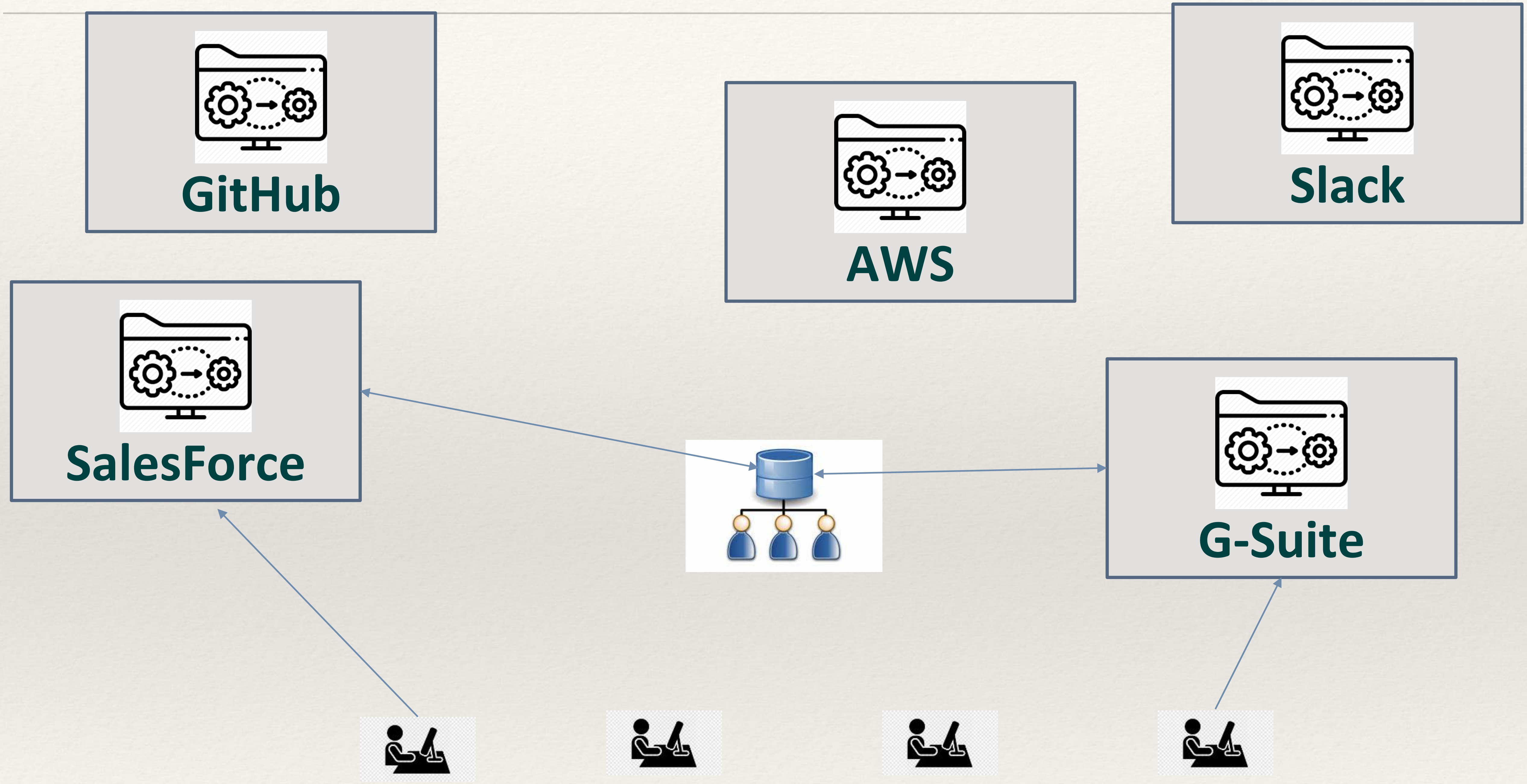
Cybersecurity will always challenge you.
But we will give you the **EDGE**.

Zero-trust based



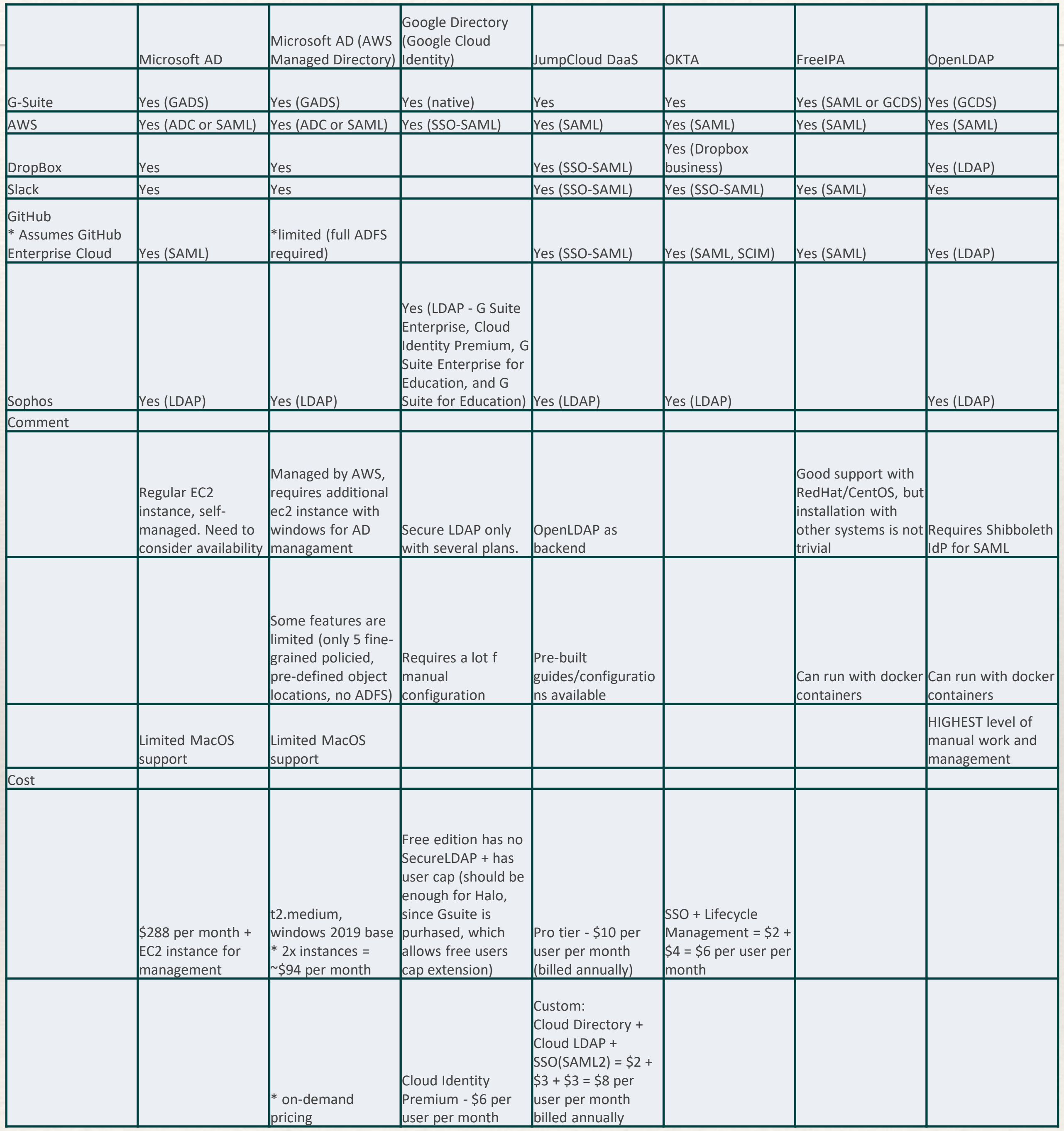
Cybersecurity will always challenge you.
But we will give you the **EDGE**.

Zero-trust based



Cybersecurity will always challenge you.
But we will give you the **EDGE**.

Zero-trust based



	Microsoft AD	Microsoft AD (AWS Managed Directory)	Google Directory (Google Cloud Identity)	JumpCloud DaaS	OKTA	FreeIPA	OpenLDAP
G-Suite	Yes (GADS)	Yes (GADS)	Yes (native)	Yes	Yes	Yes (SAML or GCDS)	Yes (GCDS)
AWS	Yes (ADC or SAML)	Yes (ADC or SAML)	Yes (SSO-SAML)	Yes (SAML)	Yes (SAML)	Yes (SAML)	Yes (SAML)
DropBox	Yes	Yes		Yes (SSO-SAML)	Yes (Dropbox business)		Yes (LDAP)
Slack	Yes	Yes		Yes (SSO-SAML)	Yes (SSO-SAML)	Yes (SAML)	Yes
GitHub * Assumes GitHub Enterprise Cloud	Yes (SAML)	*limited (full ADFS required)		Yes (SSO-SAML)	Yes (SAML, SCIM)	Yes (SAML)	Yes (LDAP)
Sophos	Yes (LDAP)	Yes (LDAP)	Yes (LDAP - G Suite Enterprise, Cloud Identity Premium, G Suite Enterprise for Education, and G Suite for Education)	Yes (LDAP)	Yes (LDAP)		Yes (LDAP)
Comment							
	Regular EC2 instance, self-managed. Need to consider availability	Managed by AWS, requires additional ec2 instance with windows for AD managament	Secure LDAP only with several plans.	OpenLDAP as backend		Good support with RedHat/CentOS, but installation with other systems is not trivial	Requires Shibboleth IdP for SAML
		Some features are limited (only 5 fine-grained policied, pre-defined object locations, no ADFS)	Requires a lot f manual configuration	Pre-built guides/configurations available		Can run with docker containers	Can run with docker containers
	Limited MacOS support	Limited MacOS support					HIGHEST level of manual work and management
Cost							
	$288 per month + EC2 instance for management	t2.medium, windows 2019 base * 2x instances = ~$94 per month	Free edition has no SecureLDAP + has user cap (should be enough for Halo, since Gsuite is purhased, which allows free users cap extension)	Pro tier - $10 per user per month (billed annually)	SSO + Lifecycle Management = $2 + $4 = $6 per user per month		
		* on-demand pricing	Cloud Identity Premium - $6 per user per month	Custom: Cloud Directory + Cloud LDAP + SSO(SAML2) = $2 + $3 + $3 = $8 per user per month billed annually			

Cybersecurity will always challenge you.
But we will give you the **EDGE**.

Information Classification

- Information classification
  - FISP
  - FISMA

Risks

- Balance, not too big, not too small
- Think of $$$
- FAIR
- Review yearly
- Produced analysis for execs, get the to understand risks.
- Measure effectiveness of mitigation
- Use risks to discuss budgets.

Incidents

- Link to Risks
- Define CIA
- Resolution definition
    - Resolution responsibility
    - Resolution verification

Policies and Procedures

- Version Control – must
- Author
- Verifier
- Approval
- View changes
- Distribution of changes
- Strong language

KPIs

- Whatever we cannot measure – we cannot manage
- Keep them simple
- Report once a year
- Keep history of the reports

Vendor Management

- Standardize audit
- SLA definition
- Contractual language

Education

- Simple but effective
- Select topics
- Hard to control

Reviews and Audits

- Hard to control
- Need tools
- Automagical artifacts/Manual artifacts
- Define procedure

BCP

- RPO
- RTO
- Maximum time before declare BCP
- System definition.

Laws and Regulations

- Local laws
- Privacy

Compliance in Public Clouds

Moving to Cloud?

1. Code Readiness
2. Configuration Readiness
3. Process Readiness

Code Readincess

OWASP:
https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content

Configuration Readiness

Through 2025, 99% of cloud security failures will be the customer’s fault.

Gartner:
https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

Configuration Readiness

CIS:
https://www.cisecurity.org/benchmark/amazon_web_services/

Processes readiness

ISO
NIST
PCI
HITRUST
OSPAR
SOC

Excersise

Create a due diligence list for 3rd party vendors

Develop your dream Cyber Security Program Effectiveness report.

HAJIME!

(Begin!)

Yahoo 2014 Breach

Reason: Spear Phishing
Intruder: Russia

The hack began with a spear-phishing email sent in early 2014 to a Yahoo company employee. It's unclear how many employees were targeted and how many emails were sent, but it only takes one person to click a link.

Once Aleksey Belan, a Latvian hacker hired by Russian agents, started poking around the network, he looked for two prizes: Yahoo's user database and the Account Management Tool, which is used to edit the database. He soon found them.
So he wouldn't lose access, he installed a backdoor on a Yahoo server that would allow him access, and in December he stole a backup copy of Yahoo's user database and transferred it to his own computer.

https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html

Yahoo hacker vs Cybersecurity Standard

Undecided

Marriot 2014 Breach

Reason: Unknown
Intruder: Possibly China

Rusty Carter, VP, Product Management, Arxan: *"In this situation, the attackers had access since 2014 which shows that for years they went undetected and were able to access sensitive data about individuals and their travel. This attack sheds light on the fact that many enterprise backend systems and databases are vulnerable because they must trust the application accessing them. Furthermore, the massive size of this breach further highlights the need for regulation to protect consumers. Companies need to protect their applications from tampering and reverse engineering attacks if they want to keep (or rebuild) their customers' trust. Key to minimizing the impact and likelihood of success is developing strategies that include strong detection and reporting of the health and status of applications both inside and outside the company's network."*

Ian Eyberg, CEO, NanoVMs: *"This breach happened because the underlying operating systems are completely broken. The underlying systems - be it Windows or Linux, the two most prevalent server-side operating systems today - are broken by design because they predate both wide-scale commercialized virtualization (a la vmware) and the "cloud" (aws). They are inherently designed to run multiple programs on the same server which is what allows attackers to run their programs on them (like connecting to a database and slurping down 500M records). This doesn't have to be the case though - newer operating systems exist that allow you to run only one program on a given virtual machine (server) - the one that was designed to run there - not the attacker's program. Hotels need to start looking at preventive measures such as only using single process systems that limit only running the single program that was designed to run on a given server thus not allowing attackers to run theirs."*

https://www.phocuswire.com/Marriott-data-breach-ex-Starwood-perspective

Marriot hackers vs Cybersecurity Standard

Undecided, would mitigate a lot of issues

Equifax 2017 Breach

Reason: Unpatched Apache

The following day, the Department of Homeland Security contacted Equifax, Experian, and TransUnion to notify them of the vulnerability. On March 9, 2017, an internal email notification was sent to Equifax administrators directing them to apply the Apache patch. Equifax's information security department ran scans on March 15, 2017 that were meant to identify systems that were vulnerable to the Apache Struts issue, but the scans did not identify the vulnerability.
The vulnerability was left unpatched until July 29, 2017 when Equifax's information security department discovered "suspicious network traffic" associated with its online dispute portal and applied the Apache patch. On July 30, 2017, Equifax observed further suspicious activity and took the web application offline. Three days letter the company hired cybersecurity firm Mandiant to conduct a forensic investigation of the breach. The investigation revealed that the data of an additional 2.5 million U.S. consumers had been breached, bringing the total number of Americans affected to approximately 145.5 million. Equifax disclosed in the same announcement that 8,000 Canadians had been impacted and stated that the forensic investigation related to UK consumers had been completed, but did not state the amount of UK consumers affected. A later announcement from Equifax stated that the data of 693,665 UK citizens were breached.

Equifax hacker vs Cybersecurity Standard

Cybersecurity Standard wins

eBay 2014 Breach

Reason: Either local disclose or brute force. Employee password compromise
Intruder: Syrian Electronic Army

eBay says the credential theft and database access occurred in late February and early March of 2014. The reason eBay didn't tell anyone before now, is because the company didn't know they had a problem. The unauthorized access was only recently discovered (early May 2014). The time between discovery and disclosure is rather short, which is a good thing.

Information on eBay was not encrypted.

https://www.eecs.yorku.ca/course_archive/2014-15/W/3482/Team3_presentation.pdf

eBay hacker vs Cybersecurity Standard

Cybersecurity Standard wins

JP Morgan Chase 2014 Breach

Reason: Remote access to an employee computer/Phishing
Intruders: Russian, Israelian hackers

"Employees often use software to tap into corporate networks from home through what are known as virtual private networks," the news report states. Chase reportedly has reset passwords used by every technology employee and disabled employee accounts that may have been compromised.

Since discovering the intrusion, some 200 employees across J.P. Morgan's technology and cybersecurity teams have worked to examine data on more than 90 servers that were compromised, sources told *The Journal*. And a core team, led by Chase's chief operating officer, Matt Zames, oversaw the bank's breach-response strategy, the paper reports.

JP Morgan Chase hacker vs Cybersecurity Standard

Cybersecurity Standard wins

Capital One 2019 Breach

Reason: Remote attack through misconfigured Web Application firewall
Intruders: Paige A. Thompson

Court documents showed that Capital One didn't learn about the hack until July 17, 2019, when someone sent a message to the company's responsible disclosure email address with a link to the GitHub page. The page had been up since April 21, with the IP address for a specific server containing the company's sensitive data.

"Capital One quickly alerted law enforcement to the data theft -- allowing the FBI to trace the intrusion," US Attorney Brian T. Moran said in a statement.

The GitHub page had Thompson's full name, as well as another page containing her resume. Court documents showed that on the resume, Thompson was listed as a systems engineer and was an employee at Amazon Web Services from 2015 to 2016. In a statement, Amazon said the former employee left the company three years before the hack took place.

https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

Capital One hacker vs Cybersecurity Standard

Cybersecurity Standard lost

Rate the day

❑ 5. Learned good amount
❑ 4. Learned some
❑ 3. Learned a bit
❑ 2. Learned nothing
❑ 1. Didn’t listen/didn’t care

Conclusion

We live in a scary world.

Is there a hope?

Maybe!

Here are my sources:

EDUCATION, KNOWLEDGE, VIGILANCE, CURIOSITY