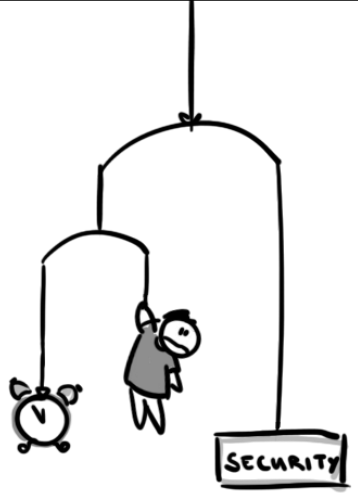
CONSTANZE DIETRICH
LEXTA Consultants Group

[@WeddingTrash // constanze.dietrich@lexta.com]

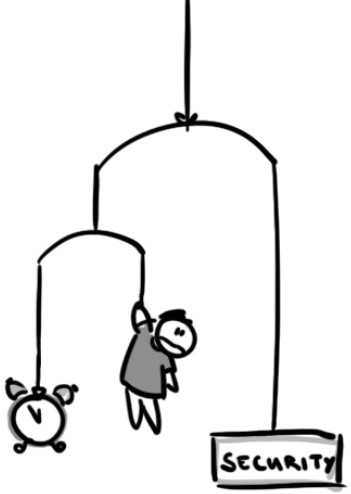


77th RIPE Meeting, Plenary Session, 16 October 2018

The Human Factors of Security Misconfigurations

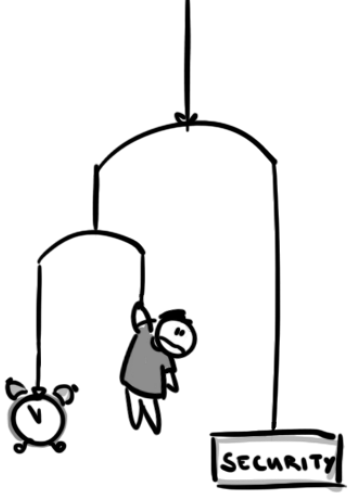
Let’s Fix the Weakest Link.


What happened?
- Beloved Defaults
- Misleading Conventions
- Troublesome Accidents
STRG+Z
RIPE 74
ripe74.ripe.net
#ripe74

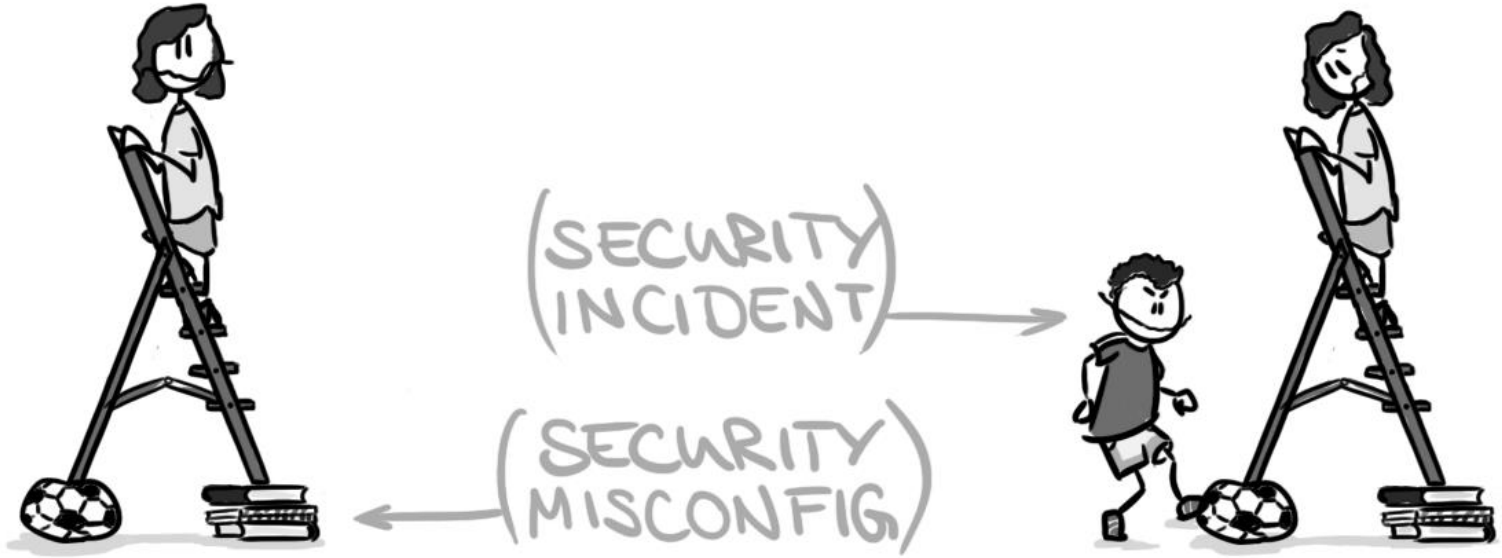

SECURITY

Outline

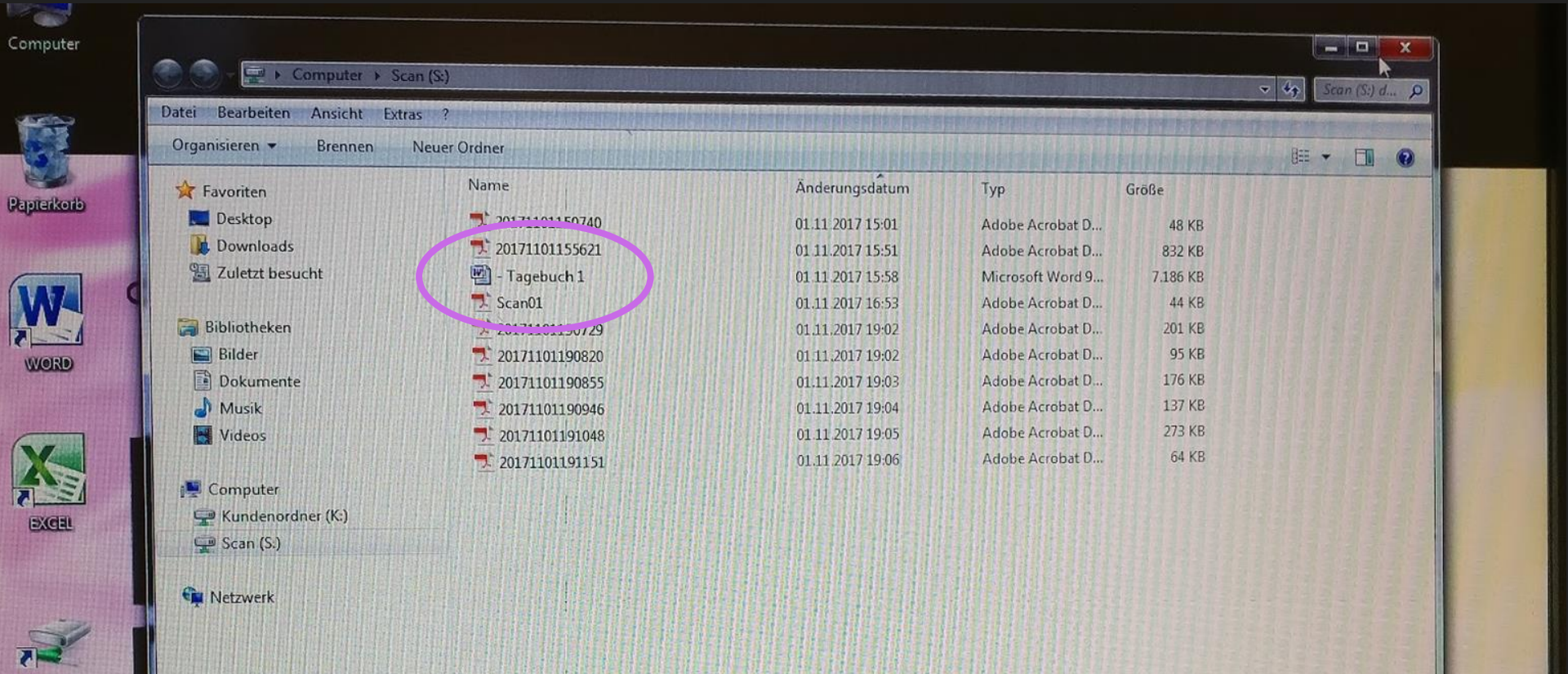
1. The issue: Security Misconfigurations
2. The method: Empirical Approach
3. The results:
   a. Who?
   b. What?
   c. Why?
   d. What else?
4. The implications: A few Ideas



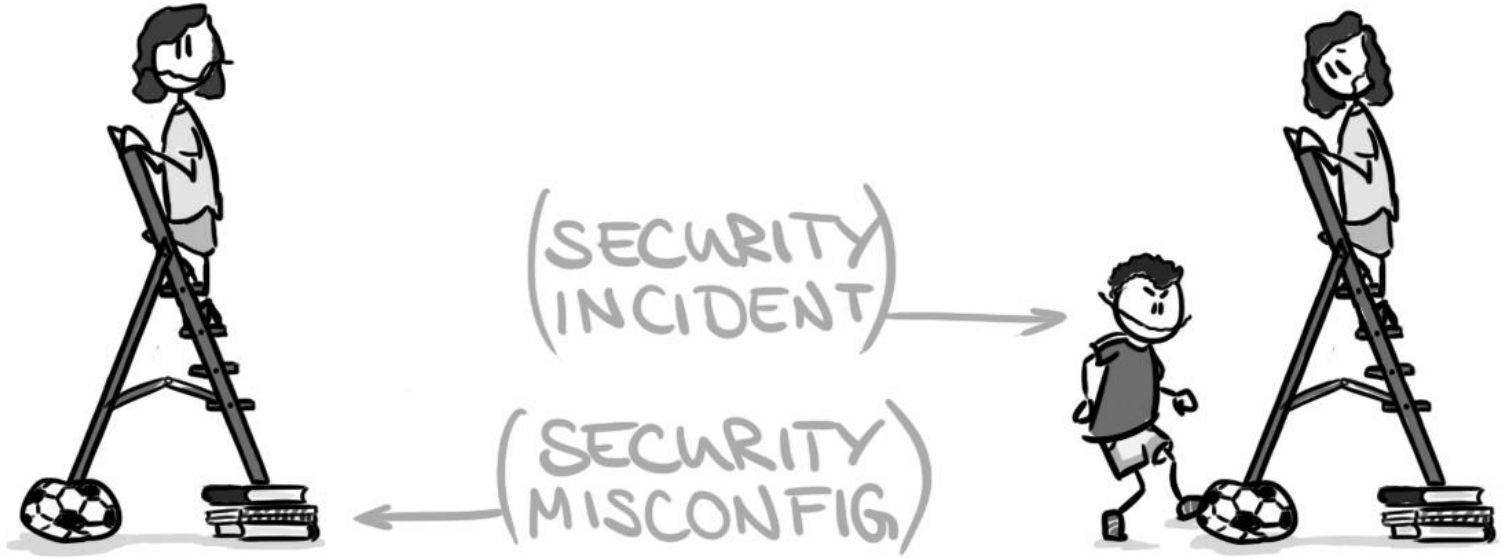
Security Misconfigurations



WTF?

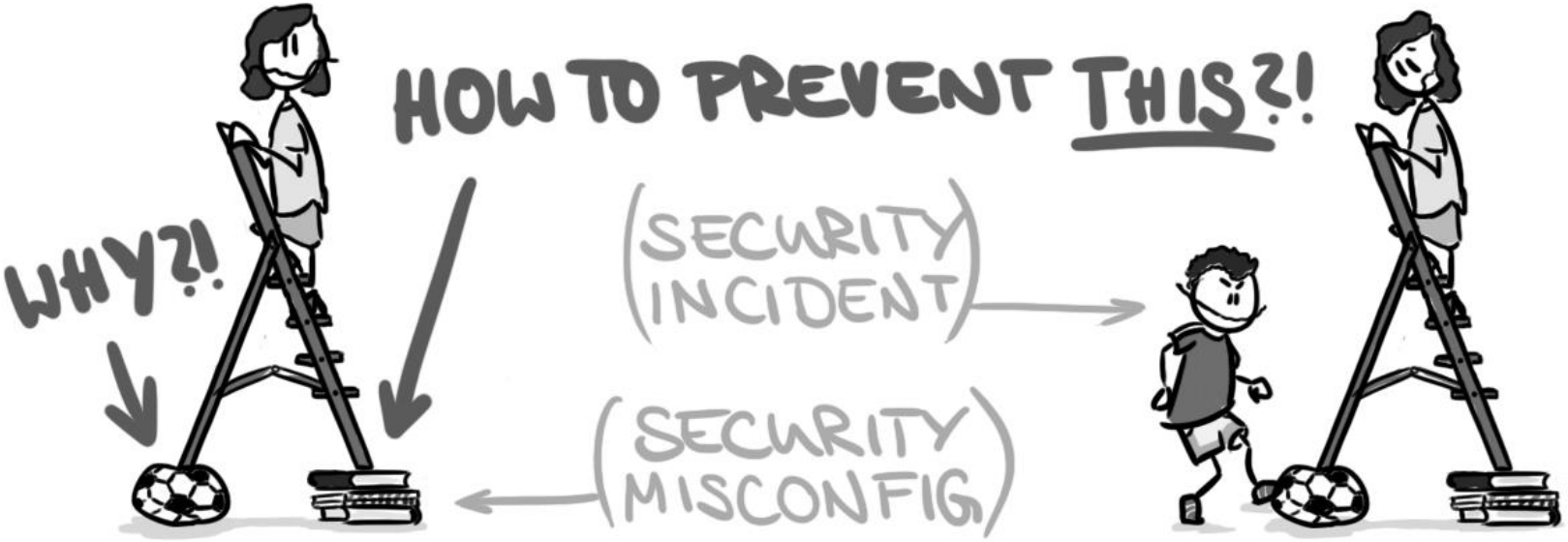

Computer
Papierkorb
WORD
EXCEL
Computer ▸ Scan (S:)
Scan (S:) d...
Datei Bearbeiten Ansicht Extras ?
Organisieren Brennen Neuer Ordner
Favoriten
Desktop
Downloads
Zuletzt besucht
Bibliotheken
Bilder
Dokumente
Musik
Videos
Computer
Kundenordner (K:)
Scan (S:)
Netzwerk
Name
Änderungsdatum
Typ
Größe
20171101155621 01.11.2017 15:51 Adobe Acrobat D... 832 KB
- Tagebuch 1 01.11.2017 15:58 Microsoft Word 9... 7.186 KB
Scan01 01.11.2017 16:53 Adobe Acrobat D... 44 KB
01.11.2017 19:02 Adobe Acrobat D... 201 KB
20171101190820 01.11.2017 19:02 Adobe Acrobat D... 95 KB
20171101190855 01.11.2017 19:03 Adobe Acrobat D... 176 KB
20171101190946 01.11.2017 19:04 Adobe Acrobat D... 137 KB
20171101191048 01.11.2017 19:05 Adobe Acrobat D... 273 KB
20171101191151 01.11.2017 19:06 Adobe Acrobat D... 64 KB

Security Misconfigurations



Security Misconfigurations

Security Misconfigurations



The Empirical Approach

(0. Presentation and Recruitment at SysAdmin Regular's Table)

1. Interviews
2. Focus Group

(2.1. Presentation of the Preliminary Findings at RIPE 74)

3. Anonymous Online Survey


9
What happened?
- Beloved Defaults
- Misleading Conventions
- Troublesome Accidents
STRG+Z
RIPE 74
ripe74.ripe.net
#ripe74

The Empirical Approach

(0. Presentation and Recruitment at SysAdmin Regular's Table)

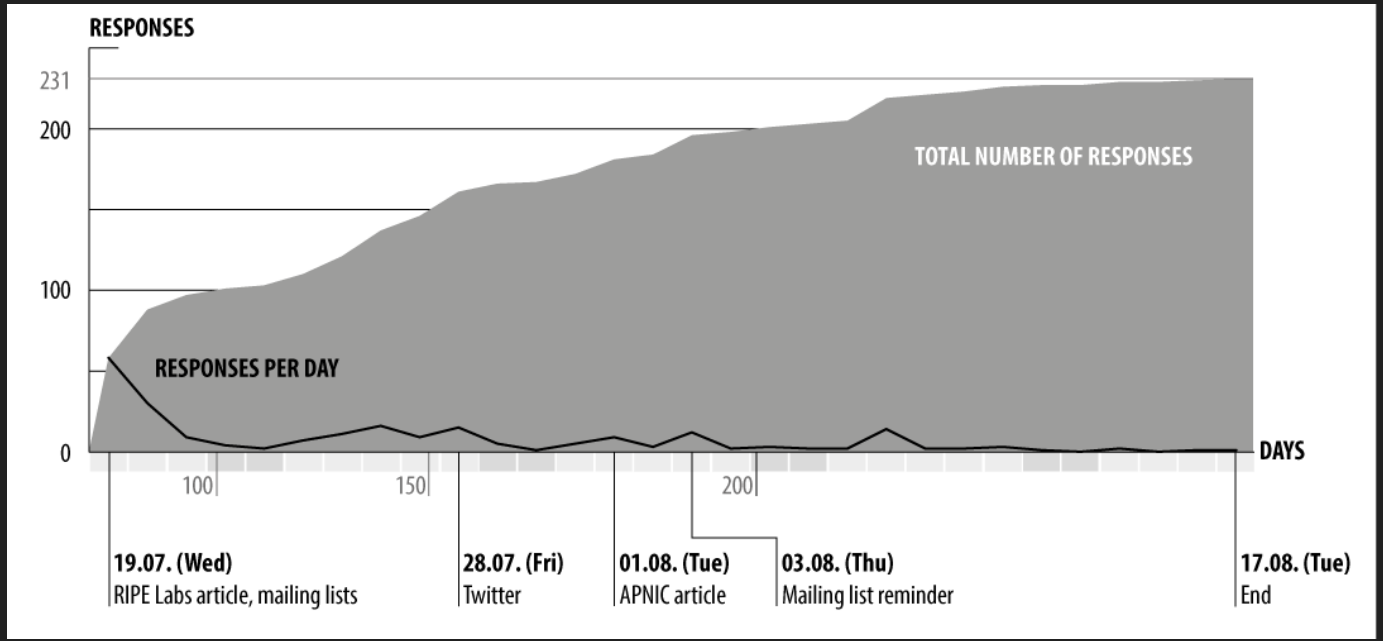
1. Interviews
2. Focus Group

(2.1. Presentation of the Preliminary Findings at RIPE 74)

3. Anonymous Online Survey

The Empirical Approach

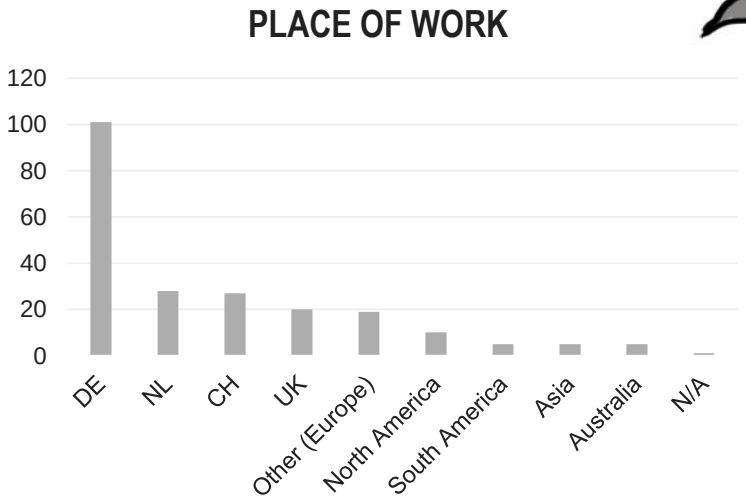
⇒ 221 valid responses in 30 days



Who?

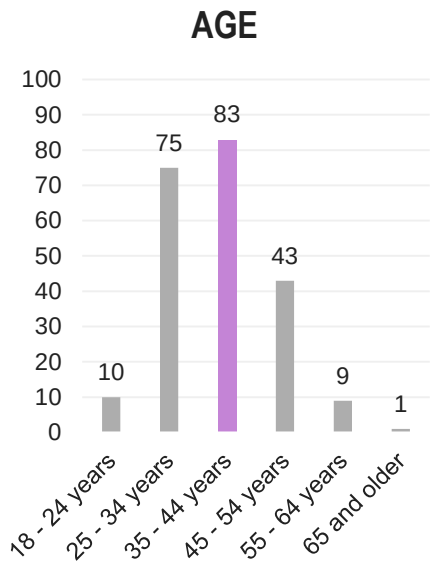
DEMOGRAPHICS

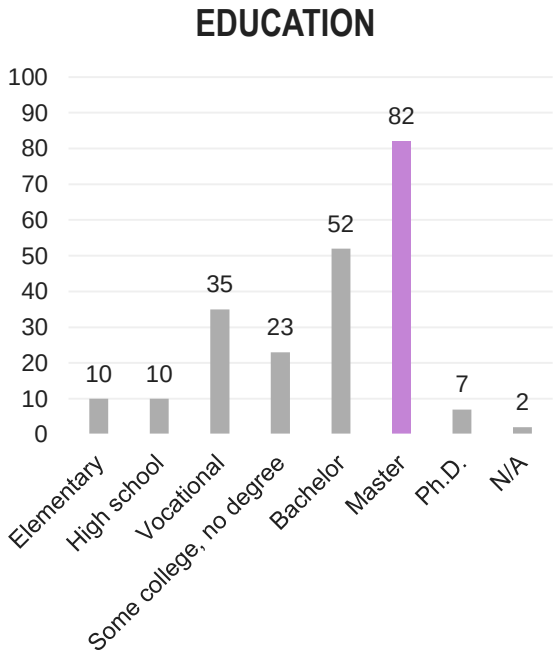
Who?

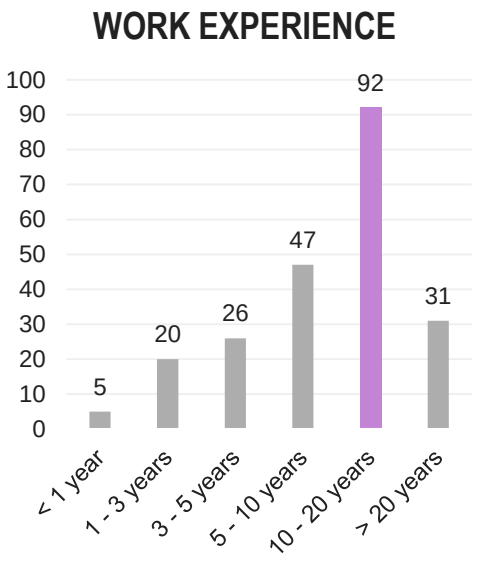

PLACE OF WORK
120
100
80
60
40
20
0
DE
NL
CH
UK
Other (Europe)
North America
South America
Asia
Australia
N/A


195
10
5
5
5

Who?


AGE
100
90
80
70
60
50
40
30
20
10
0
10
75
83
43
9
1
18 - 24 years
25 - 34 years
35 - 44 years
45 - 54 years
55 - 64 years
65 and older

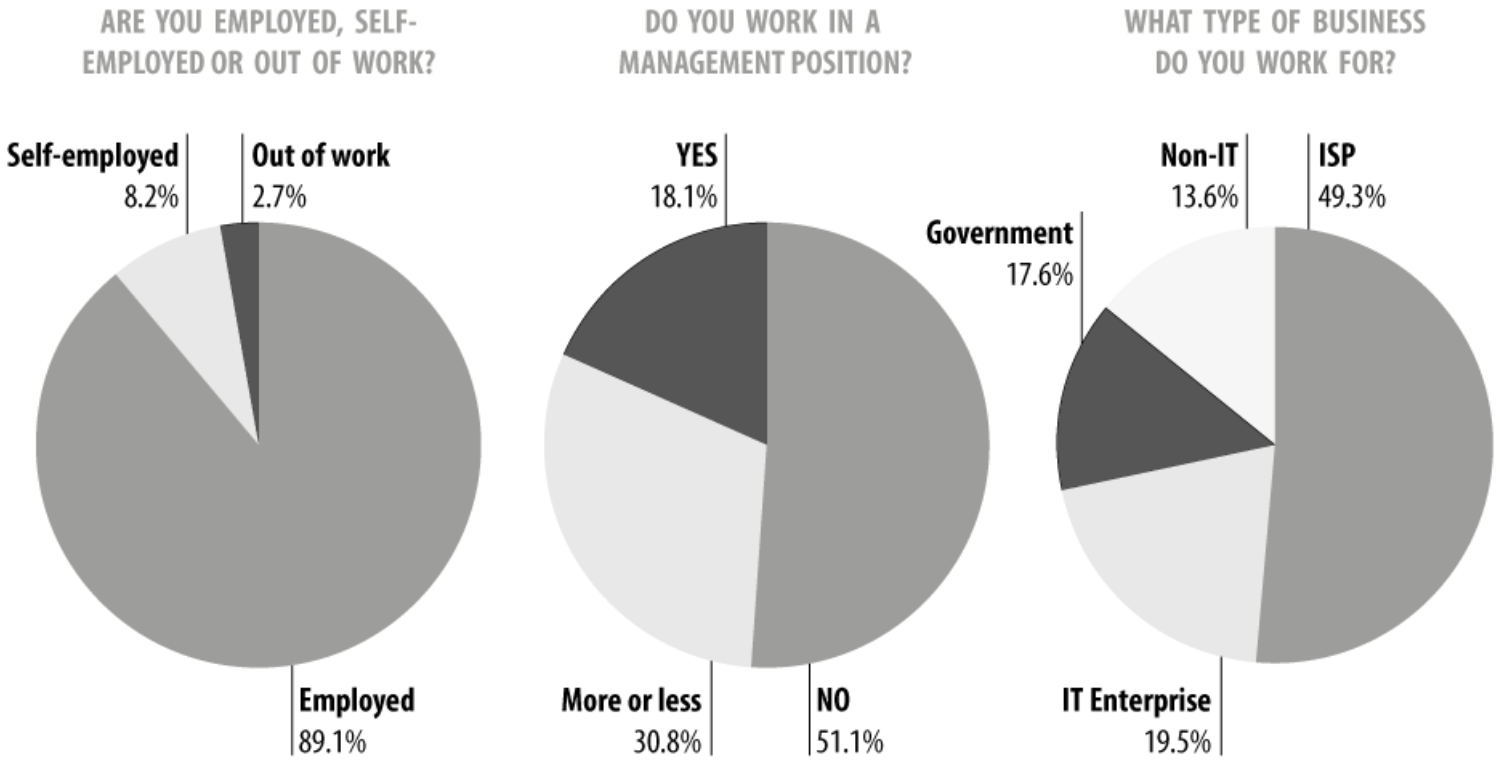

EDUCATION
100
90
80
70
60
50
40
30
20
10
0
10
10
35
23
52
82
7
2
Elementary
High school
Vocational
Some college, no degree
Bachelor
Master
Ph.D.
N/A


WORK EXPERIENCE
100
90
80
70
60
50
40
30
20
10
0
5
20
26
47
92
31
< 1 year
1 - 3 years
3 - 5 years
5 - 10 years
10 - 20 years
> 20 years

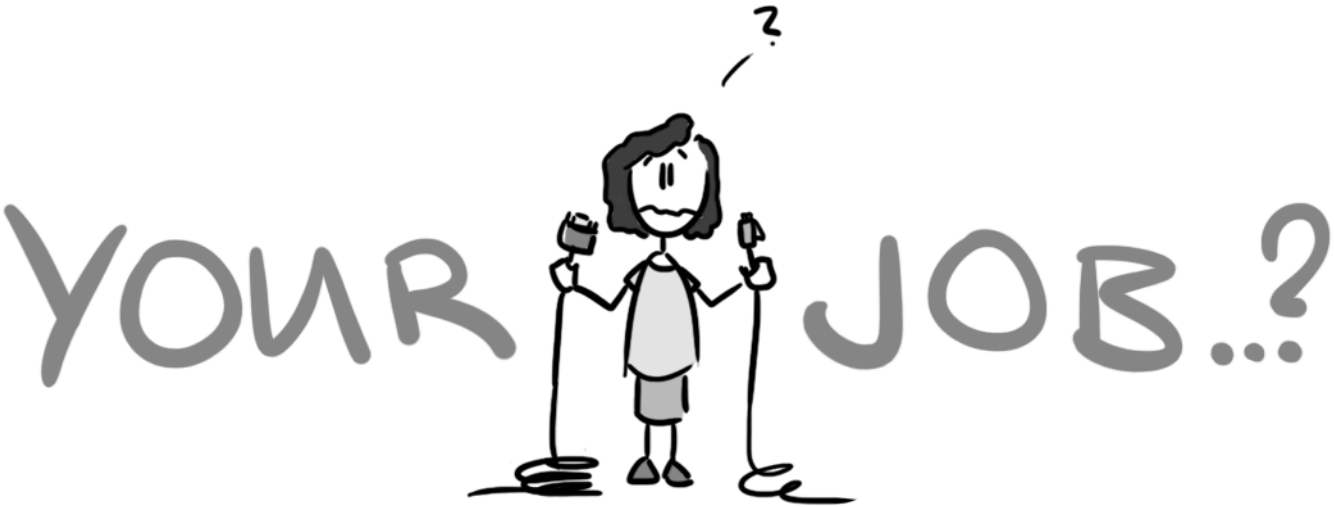
Who?

Who?

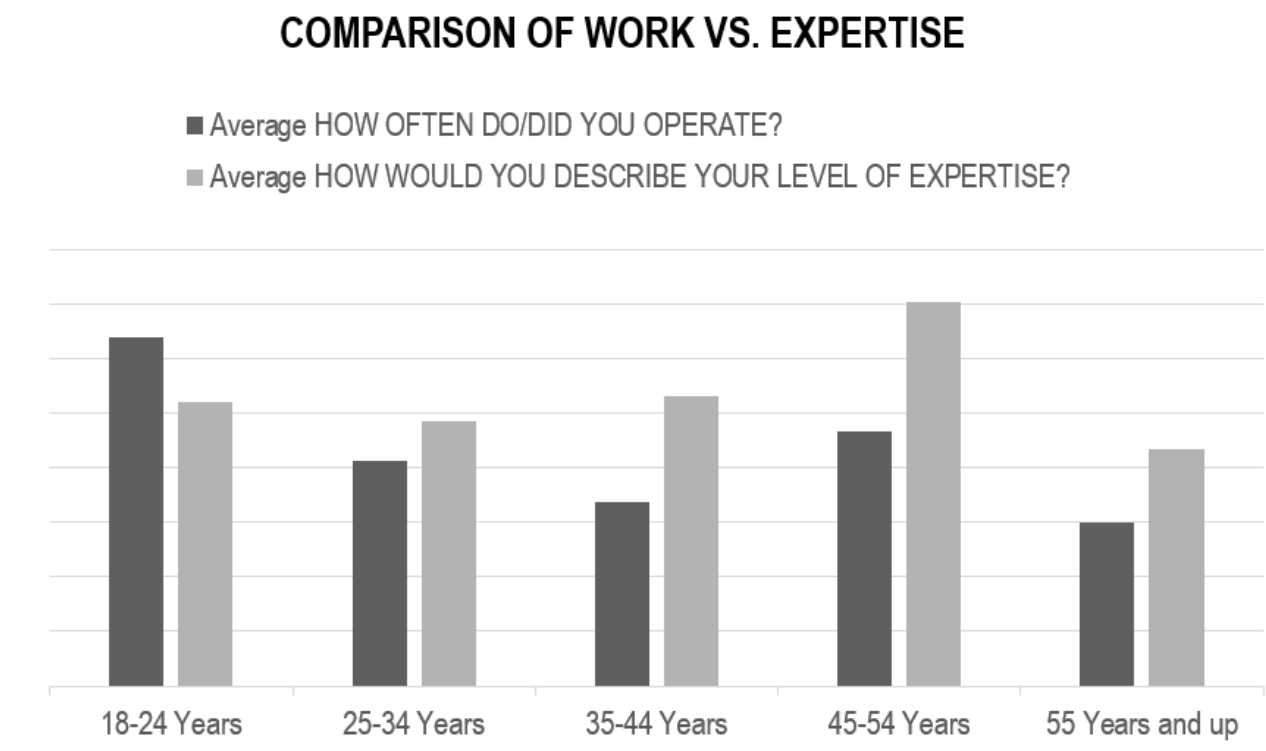
JOBS


ARE YOU EMPLOYED, SELF-EMPLOYED OR OUT OF WORK?
Self-employed 8.2%
Out of work 2.7%
Employed 89.1%
DO YOU WORK IN A MANAGEMENT POSITION?
YES 18.1%
More or less 30.8%
NO 51.1%
WHAT TYPE OF BUSINESS DO YOU WORK FOR?
Non-IT 13.6%
ISP 49.3%
Government 17.6%
IT Enterprise 19.5%

Who?



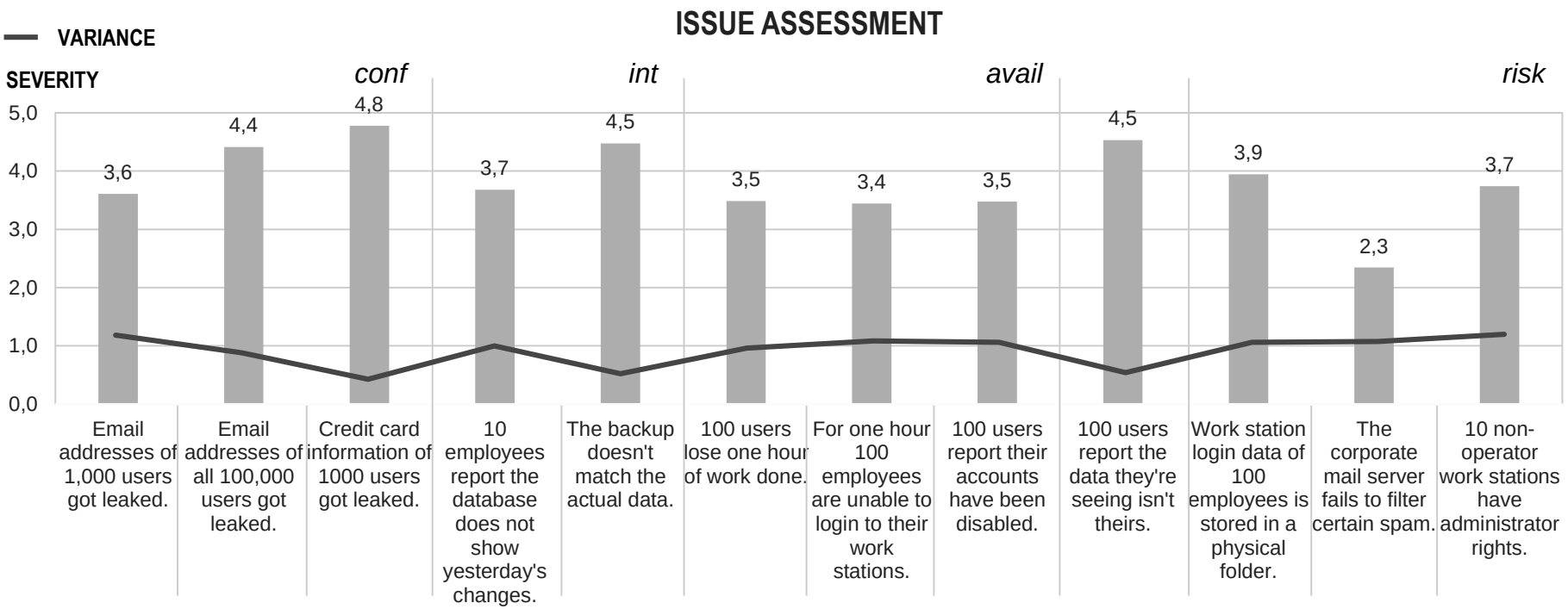
Who?


COMPARISON OF WORK VS. EXPERTISE
Average HOW OFTEN DO/DID YOU OPERATE?
Average HOW WOULD YOU DESCRIBE YOUR LEVEL OF EXPERTISE?
18-24 Years
25-34 Years
35-44 Years
45-54 Years
55 Years and up

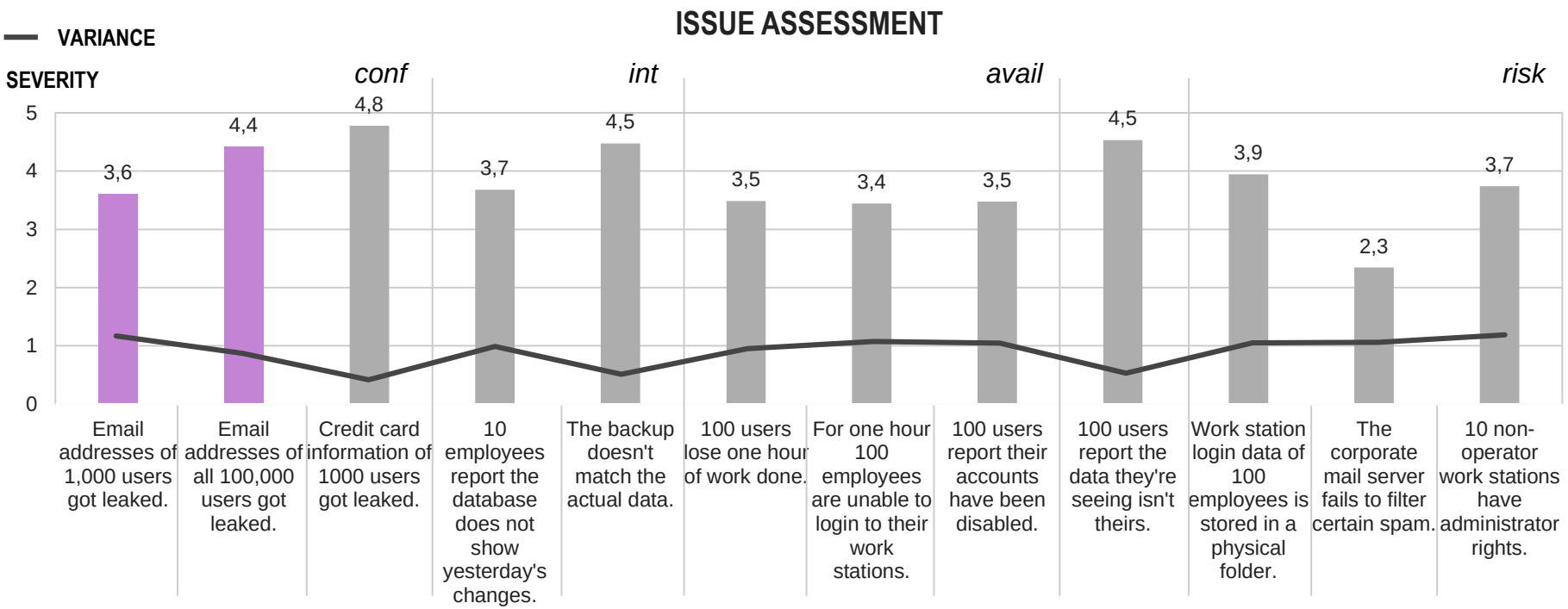
Who?

ISSUES

What?

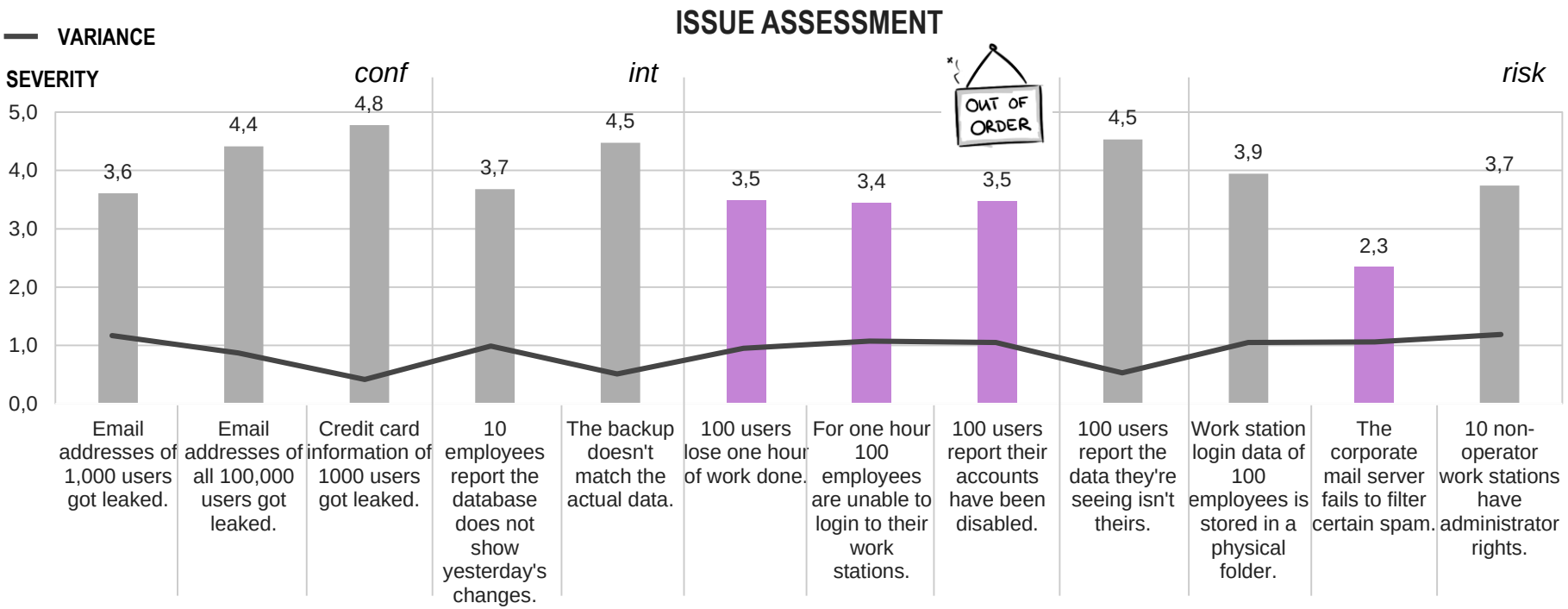

ISSUE ASSESSMENT
VARIANCE
SEVERITY
conf
int
avail
risk
5,0
4,0
3,0
2,0
1,0
0,0
3,6
4,4
4,8
3,7
4,5
3,5
3,4
3,5
4,5
3,9
2,3
3,7
Email addresses of 1,000 users got leaked.
Email addresses of all 100,000 users got leaked.
Credit card information of 1000 users got leaked.
10 employees report the database does not show yesterday's changes.
The backup doesn't match the actual data.
100 users lose one hour of work done.
For one hour 100 employees are unable to login to their work stations.
100 users report their accounts have been disabled.
100 users report the data they're seeing isn't theirs.
Work station login data of 100 employees is stored in a physical folder.
The corporate mail server fails to filter certain spam.
10 non-operator work stations have administrator rights.

What?



5 Critical; 4 High; 3 Medium; 2 Low; 1 Very low

What?

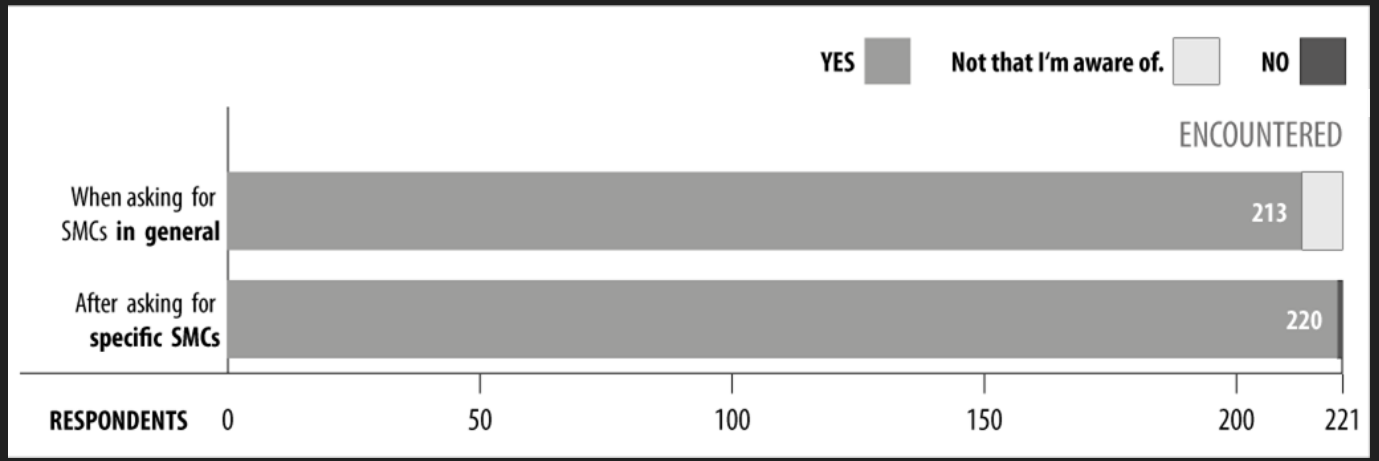

ISSUE ASSESSMENT
VARIANCE
SEVERITY
conf
int
risk
OUT OF ORDER
5,0
4,0
3,0
2,0
1,0
0,0
3,6
4,4
4,8
3,7
4,5
3,5
3,4
3,5
4,5
3,9
2,3
3,7
Email addresses of 1,000 users got leaked.
Email addresses of all 100,000 users got leaked.
Credit card information of 1000 users got leaked.
10 employees report the database does not show yesterday's changes.
The backup doesn't match the actual data.
100 users lose one hour of work done.
For one hour 100 employees are unable to login to their work stations.
100 users report their accounts have been disabled.
100 users report the data they're seeing isn't theirs.
Work station login data of 100 employees is stored in a physical folder.
The corporate mail server fails to filter certain spam.
10 non-operator work stations have administrator rights.

What?


EXPERIENCES
(SECURITY INCIDENT)→
←(SECURITY MISCONFIGURATION)

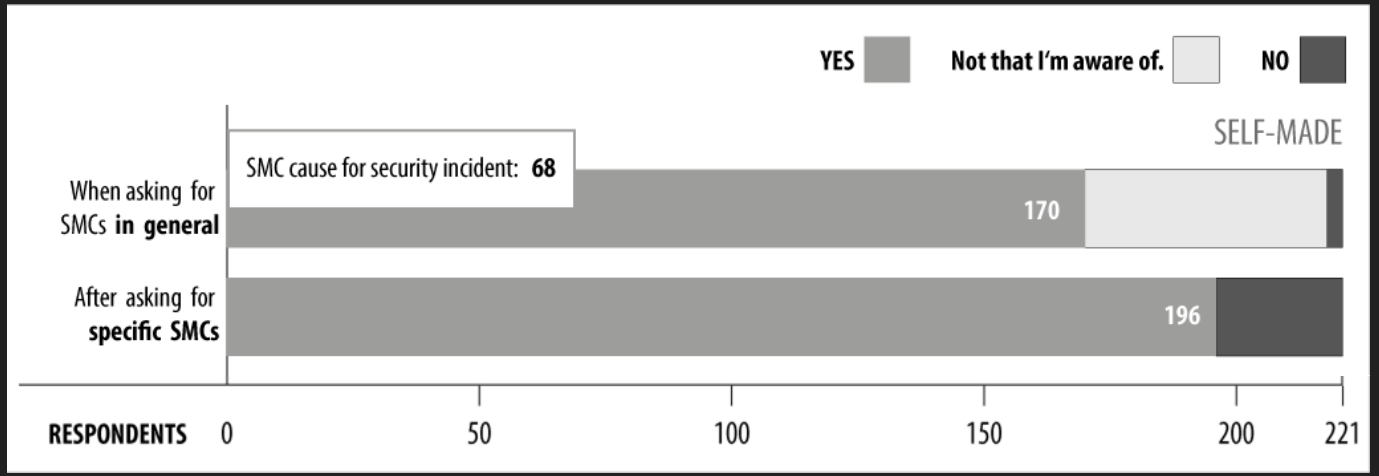
What?

220 operators have encountered security misconfigrations:

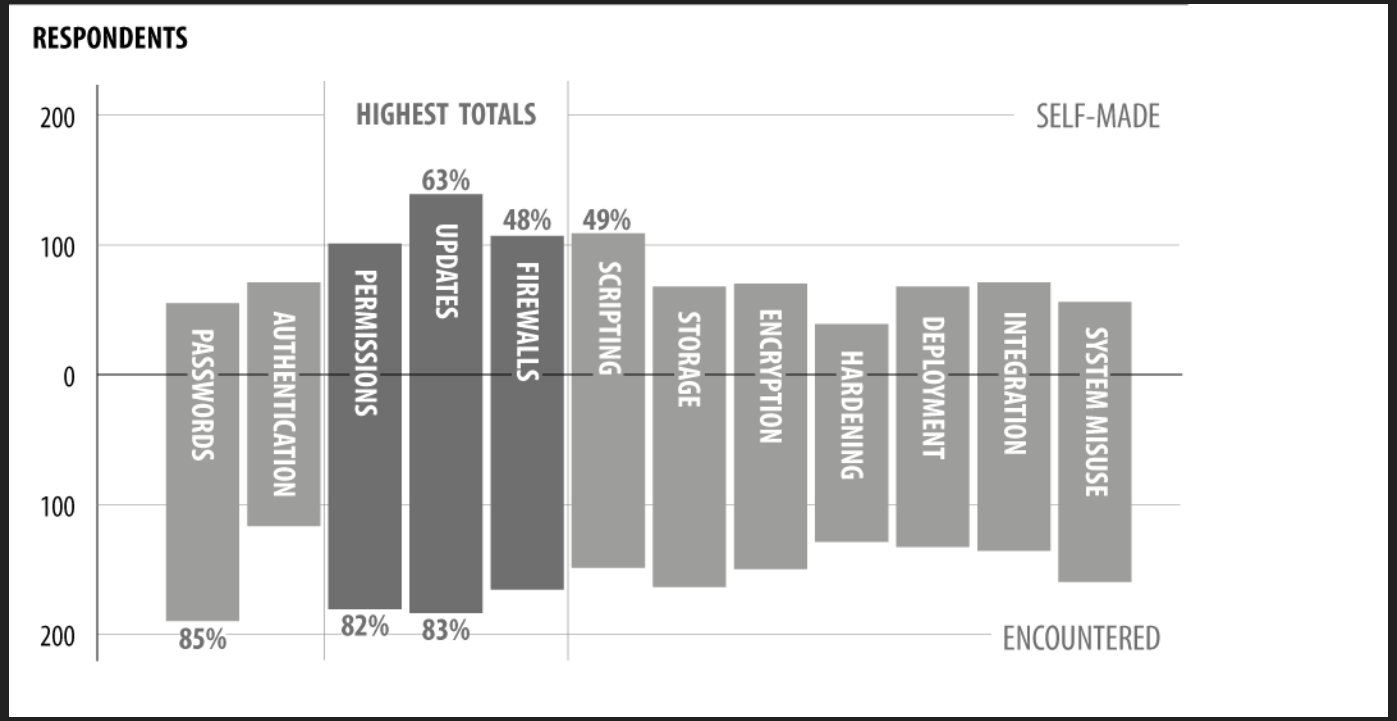


What?

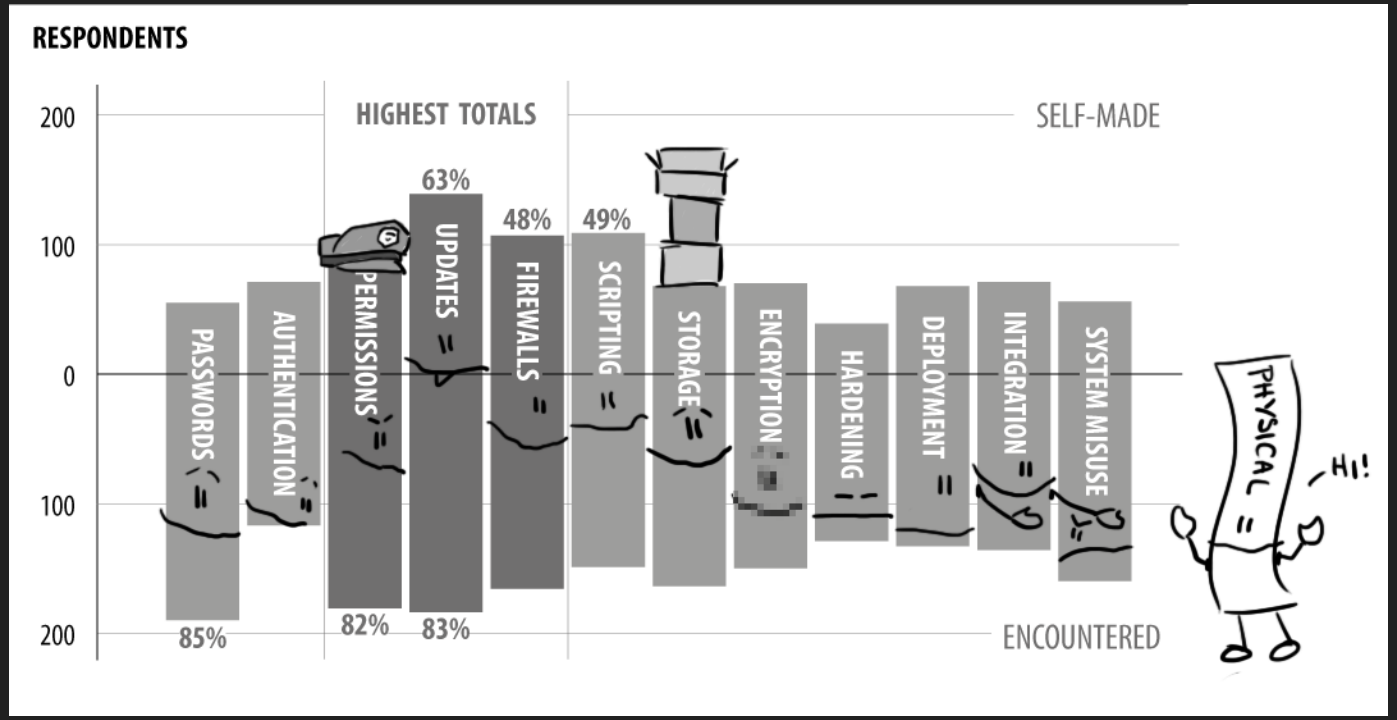
196 operators made security misconfigurations



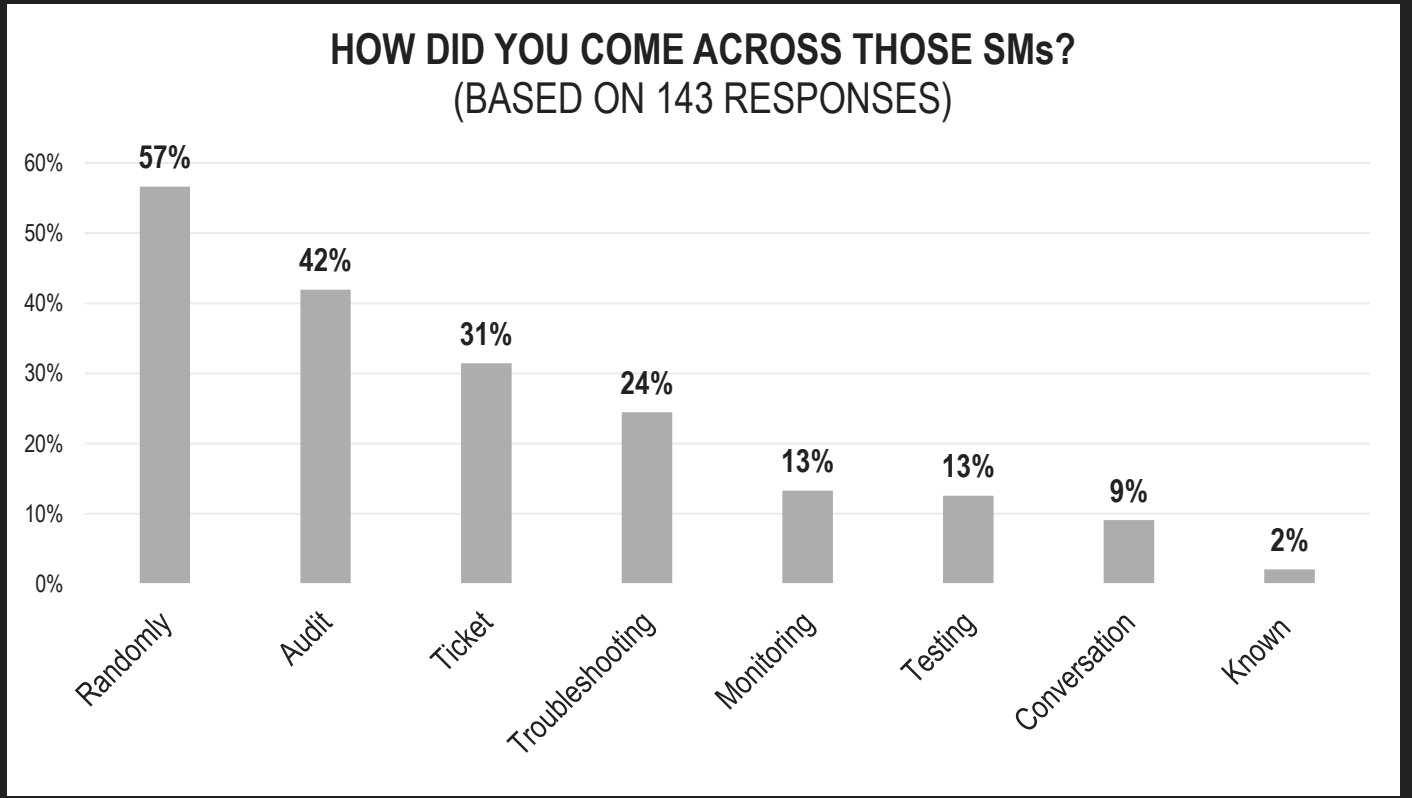
What?


RESPONDENTS
HIGHEST TOTALS
SELF-MADE
ENCOUNTERED
200
100
0
100
200
PASSWORDS
AUTHENTICATION
PERMISSIONS
UPDATES
FIREWALLS
SCRIPTING
STORAGE
ENCRYPTION
HARDENING
DEPLOYMENT
INTEGRATION
SYSTEM MISUSE
85%
82%
83%
63%
48%
49%

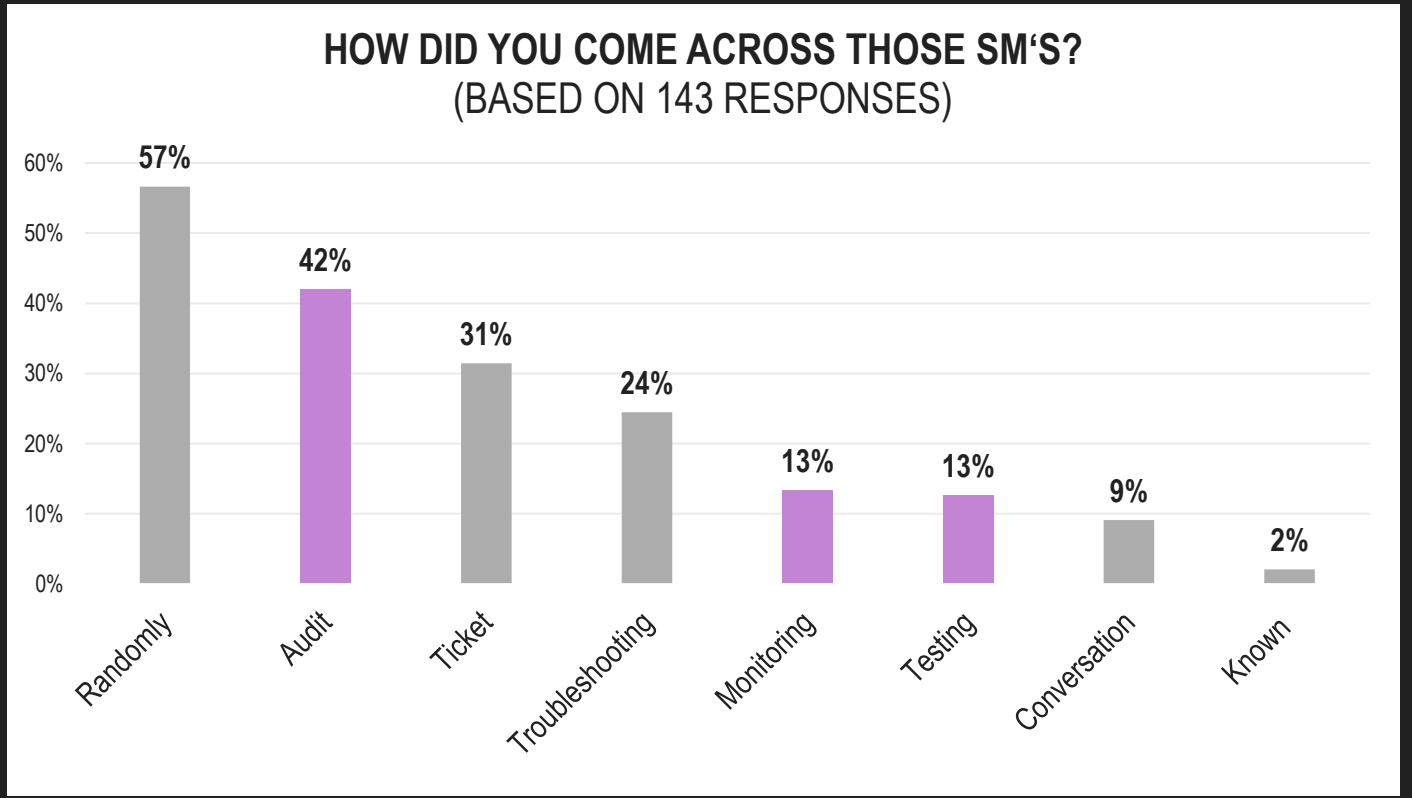
What?


RESPONDENTS
HIGHEST TOTALS
SELF-MADE
ENCOUNTERED
200
100
0
100
200
PASSWORDS
AUTHENTICATION
PERMISSIONS
UPDATES
FIREWALLS
SCRIPTING
STORAGE
ENCRYPTION
HARDENING
DEPLOYMENT
INTEGRATION
SYSTEM MISUSE
85%
82%
83%
63%
48%
49%
PHYSICAL
HI!

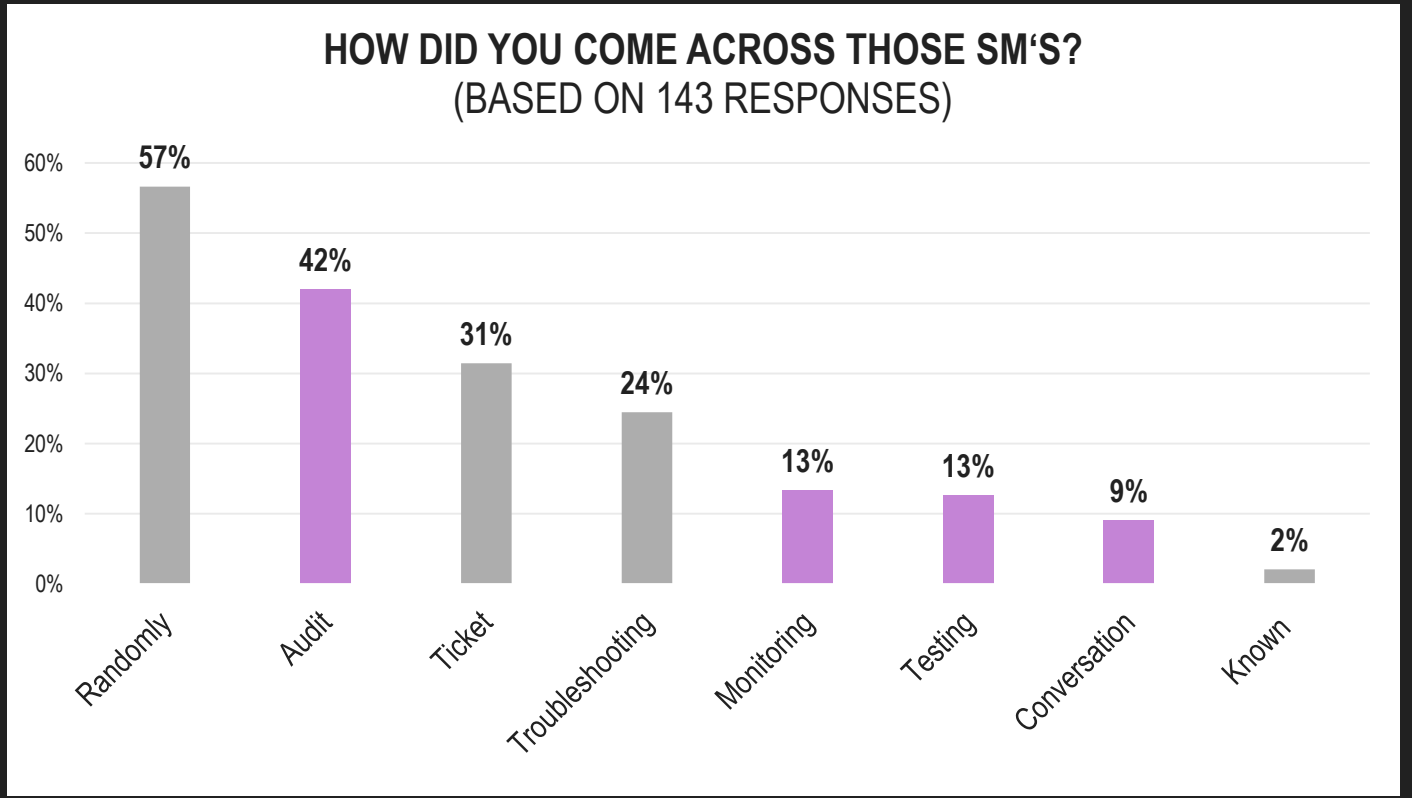
How?


HOW DID YOU COME ACROSS THOSE SMs?
(BASED ON 143 RESPONSES)
60%
50%
40%
30%
20%
10%
0%
57%
42%
31%
24%
13%
13%
9%
2%
Randomly
Audit
Ticket
Troubleshooting
Monitoring
Testing
Conversation
Known

How?

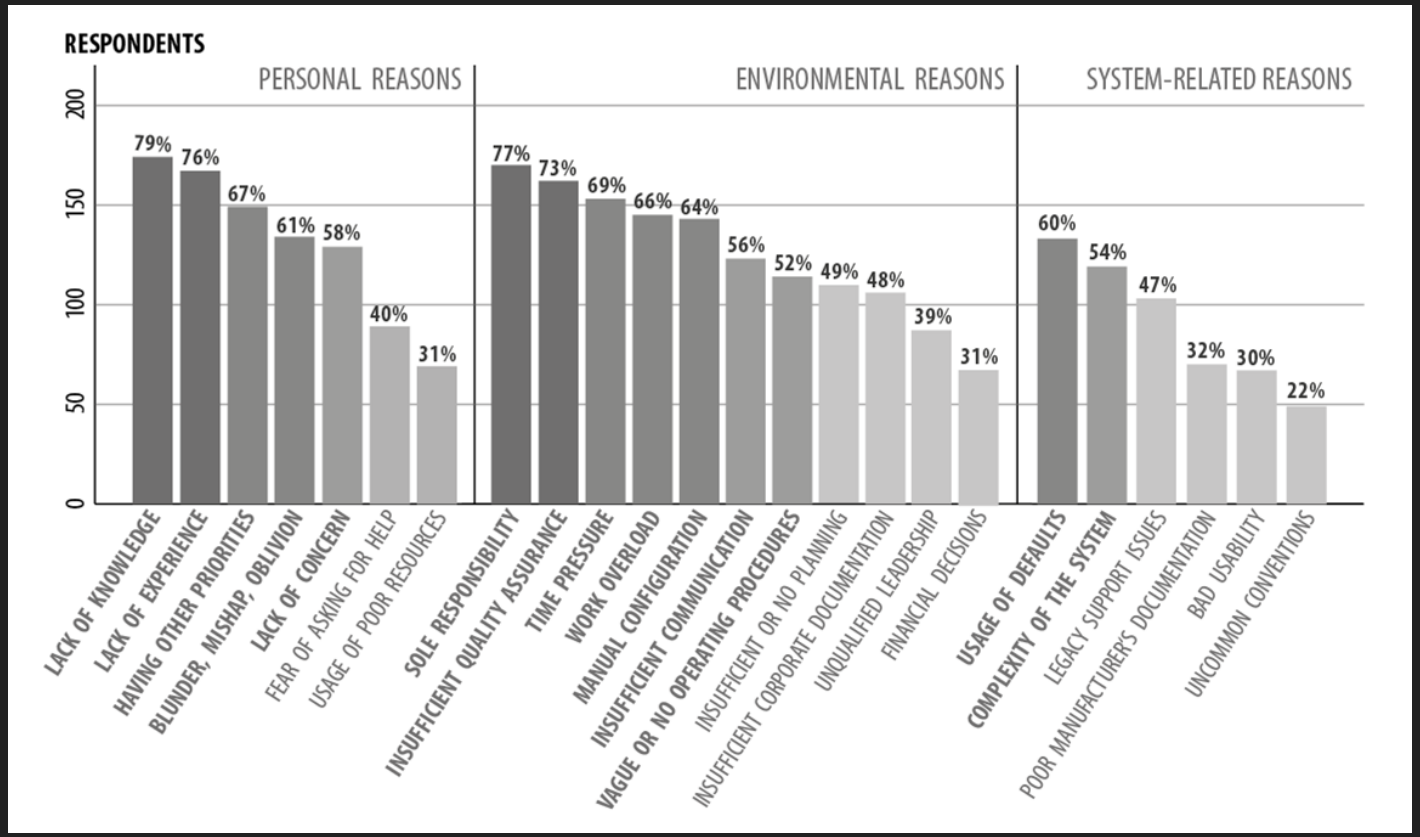

HOW DID YOU COME ACROSS THOSE SM‘S?
(BASED ON 143 RESPONSES)
60%
50%
40%
30%
20%
10%
0%
57%
42%
31%
24%
13%
13%
9%
2%
Randomly
Audit
Ticket
Troubleshooting
Monitoring
Testing
Conversation
Known

How?

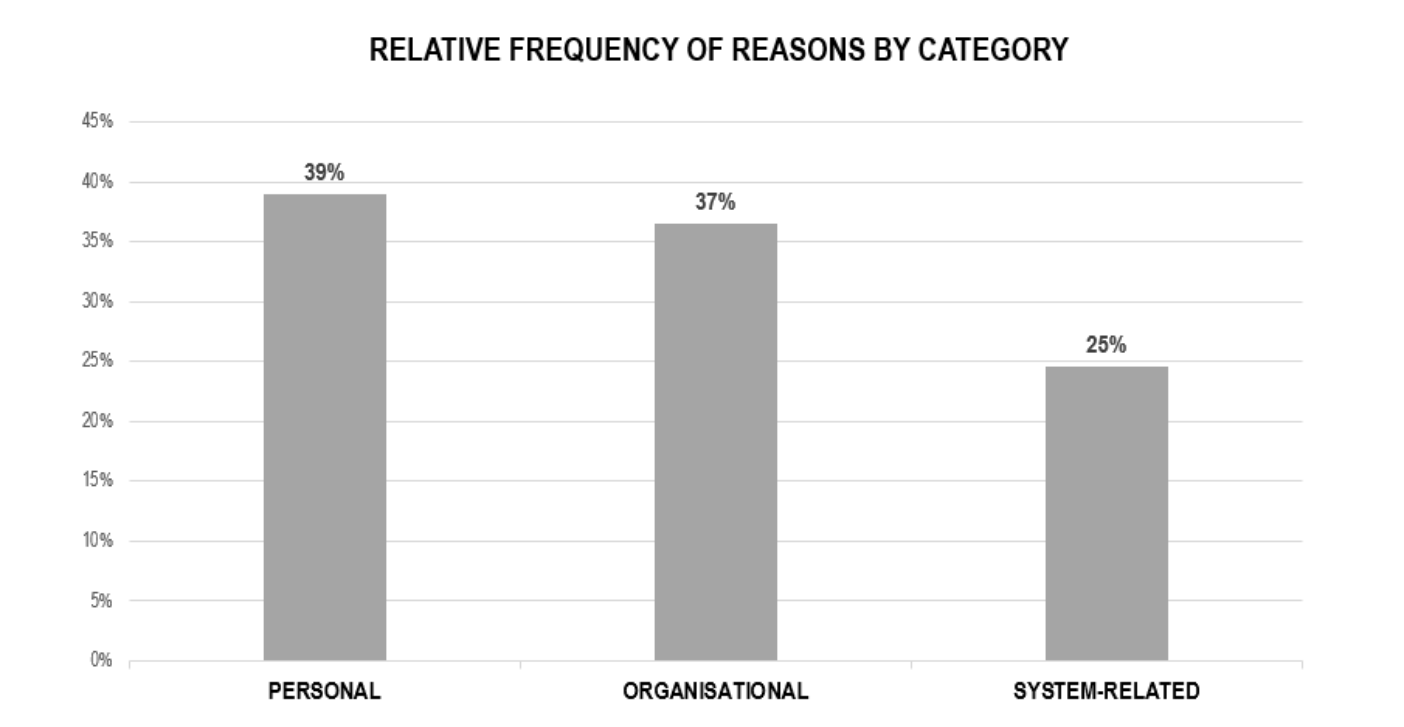

HOW DID YOU COME ACROSS THOSE SM‘S?
(BASED ON 143 RESPONSES)
60%
50%
40%
30%
20%
10%
0%
57%
42%
31%
24%
13%
13%
9%
2%
Randomly
Audit
Ticket
Troubleshooting
Monitoring
Testing
Conversation
Known

Why?

Why?


RESPONDENTS
PERSONAL REASONS
ENVIRONMENTAL REASONS
SYSTEM-RELATED REASONS
0
50
100
150
200
79%
76%
67%
61%
58%
40%
31%
77%
73%
69%
66%
64%
56%
52%
49%
48%
39%
31%
60%
54%
47%
32%
30%
22%
LACK OF KNOWLEDGE
LACK OF EXPERIENCE
HAVING OTHER PRIORITIES
BLUNDER, MISHAP, OBLIVION
LACK OF CONCERN
FEAR OF ASKING FOR HELP
USAGE OF POOR RESOURCES
SOLE RESPONSIBILITY
INSUFFICIENT QUALITY ASSURANCE
TIME PRESSURE
WORK OVERLOAD
MANUAL CONFIGURATION
INSUFFICIENT COMMUNICATION
VAGUE OR NO OPERATING PROCEDURES
INSUFFICIENT OR NO PLANNING
INSUFFICIENT CORPORATE DOCUMENTATION
UNQUALIFIED LEADERSHIP
FINANCIAL DECISIONS
USAGE OF DEFAULTS
COMPLEXITY OF THE SYSTEM
LEGACY SUPPORT ISSUES
POOR MANUFACTURER'S DOCUMENTATION
BAD USABILITY
UNCOMMON CONVENTIONS

Why?

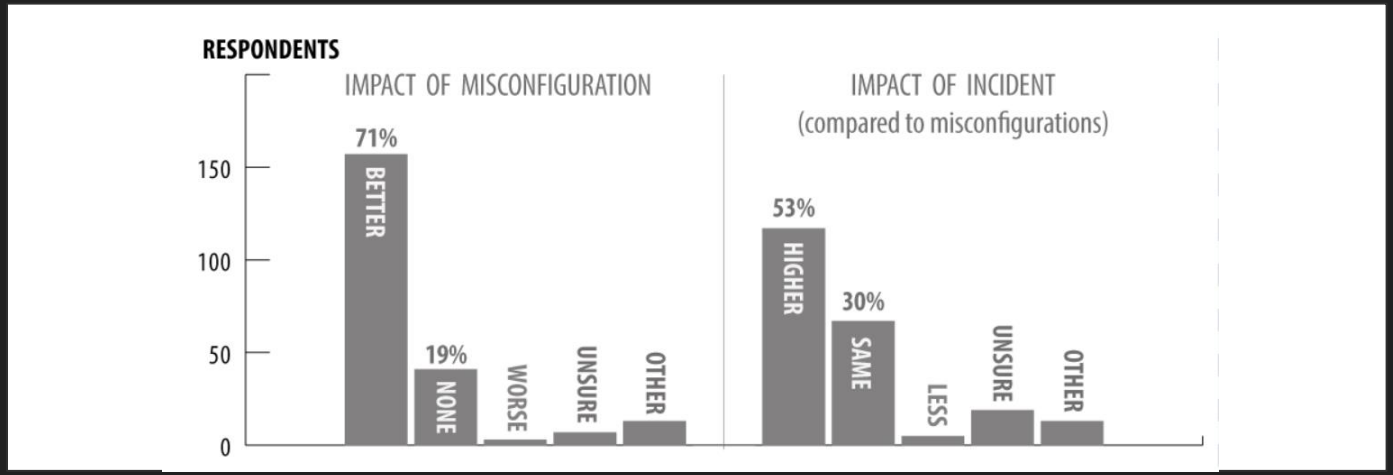

RELATIVE FREQUENCY OF REASONS BY CATEGORY
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
39%
37%
25%
PERSONAL
ORGANISATIONAL
SYSTEM-RELATED

What else?

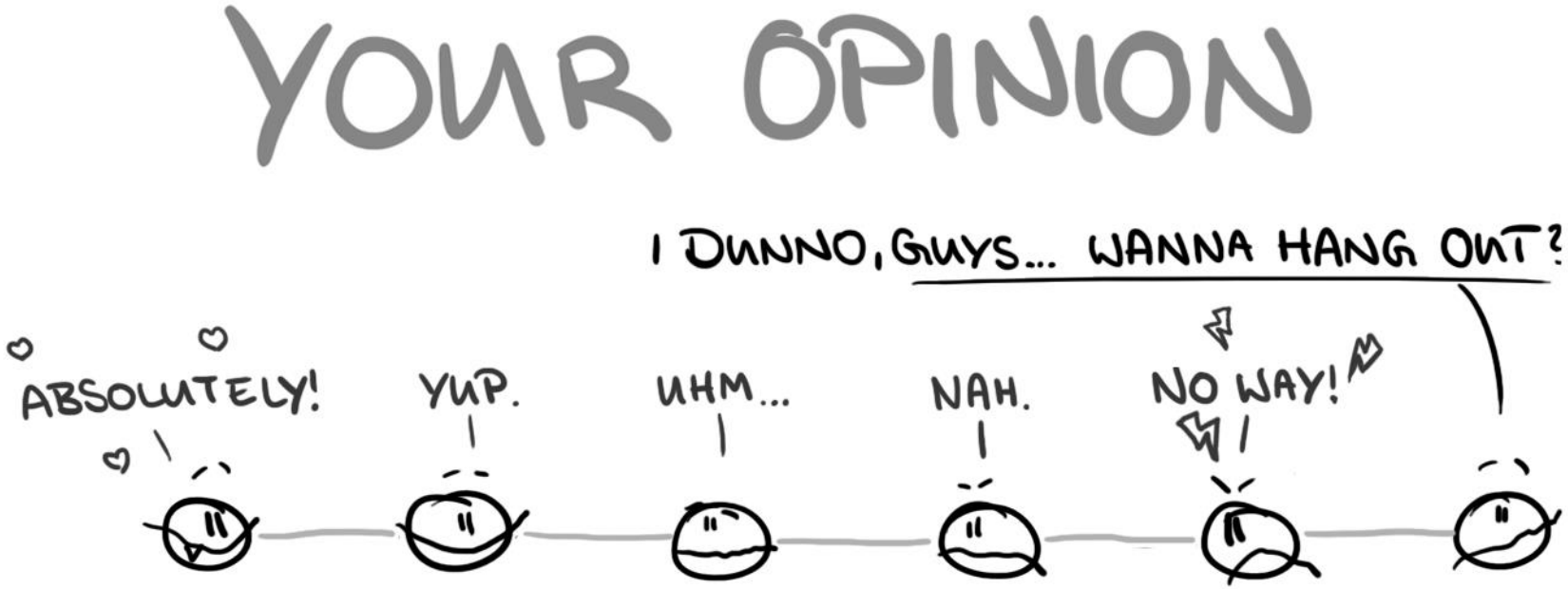
REACTIONS

What else?

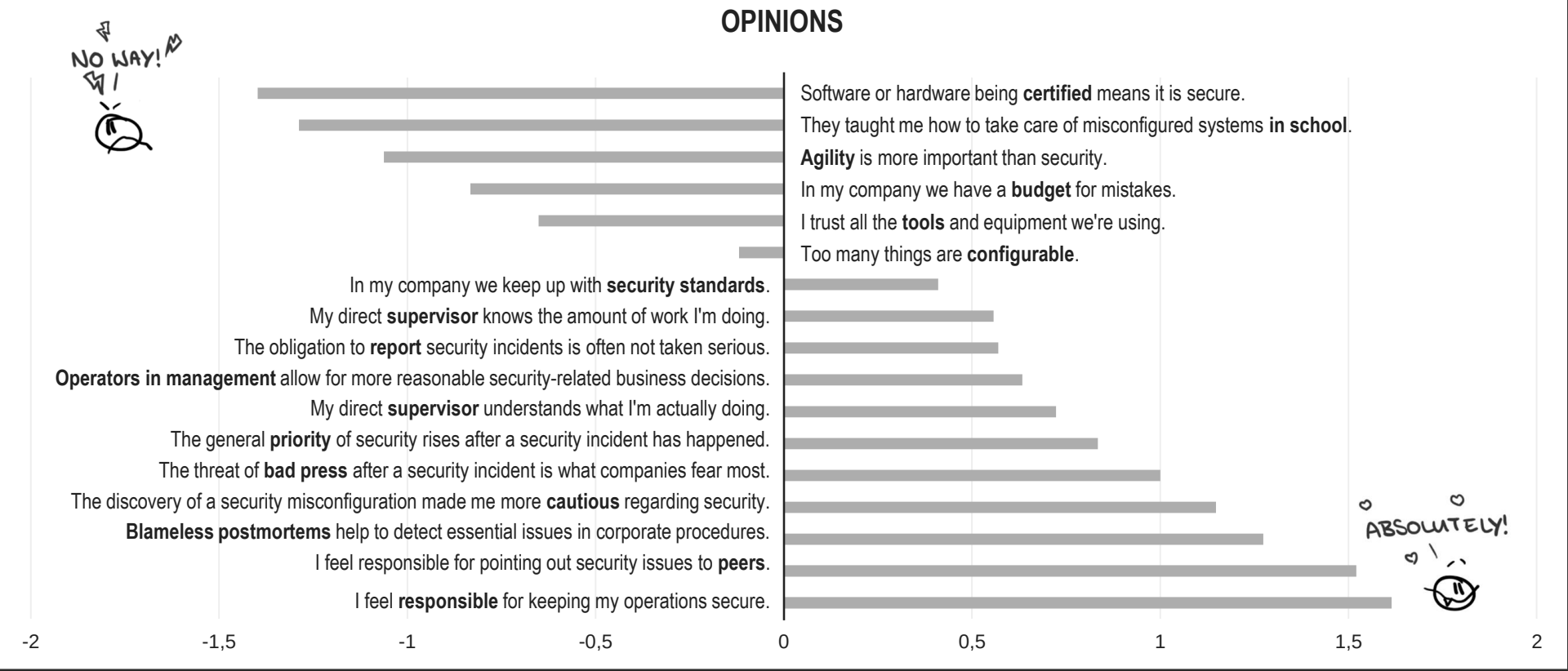
“One incident gets your boss to improve security.
Two incidents gets their boss to improve security.
Three.... You get it, don't you?”
− respondent #120



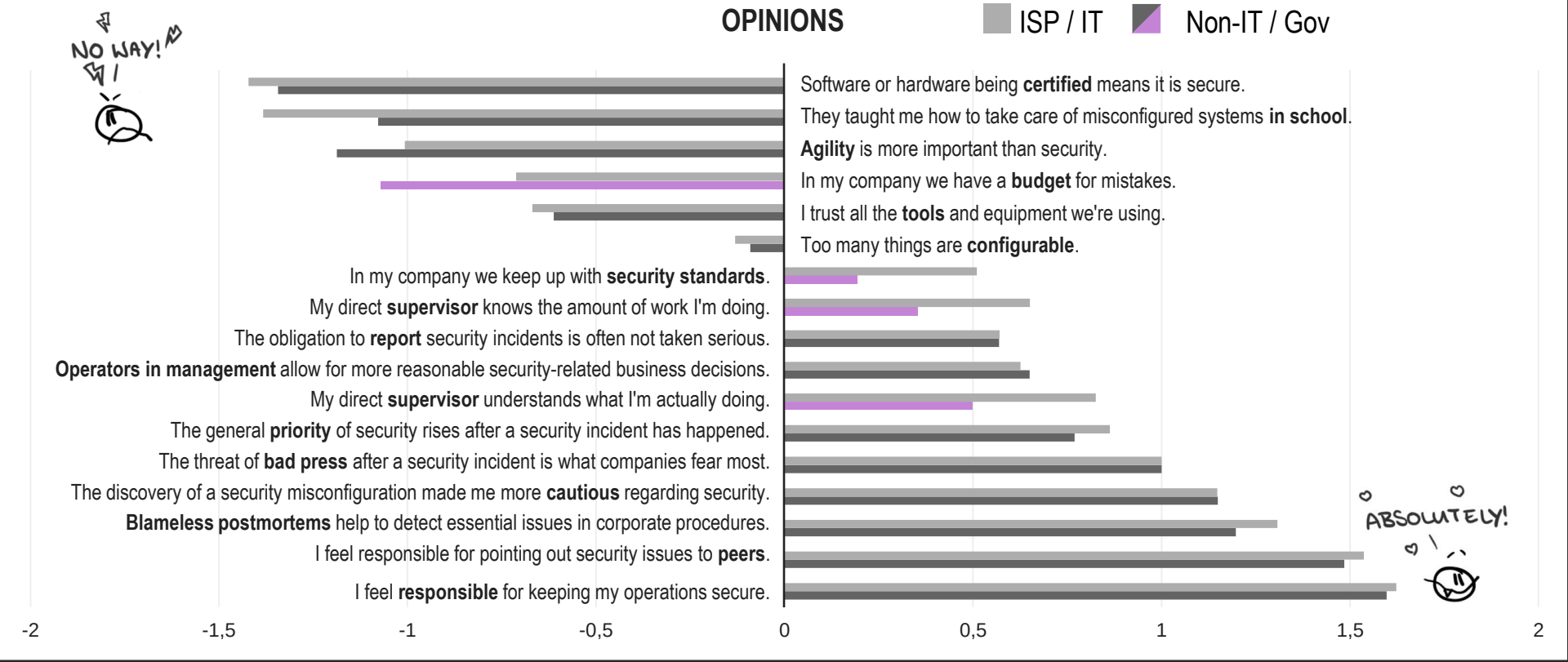
What else?


YOUR OPINION
I DUNNO, GUYS... WANNA HANG OUT?
ABSOLUTELY!
YUP.
UHM...
NAH.
NO WAY!

What else?


OPINIONS
NO WAY!
ABSOLUTELY!
Software or hardware being **certified** means it is secure.
They taught me how to take care of misconfigured systems **in school**.
Agility is more important than security.
In my company we have a **budget** for mistakes.
I trust all the **tools** and equipment we're using.
Too many things are **configurable**.
In my company we keep up with **security standards**.
My direct **supervisor** knows the amount of work I'm doing.
The obligation to **report** security incidents is often not taken serious.
Operators in management allow for more reasonable security-related business decisions.
My direct **supervisor** understands what I'm actually doing.
The general **priority** of security rises after a security incident has happened.
The threat of **bad press** after a security incident is what companies fear most.
The discovery of a security misconfiguration made me more **cautious** regarding security.
Blameless postmortems help to detect essential issues in corporate procedures.
I feel responsible for pointing out security issues to **peers**.
I feel **responsible** for keeping my operations secure.
-2
-1,5
-1
-0,5
0
0,5
1
1,5
2

What else?

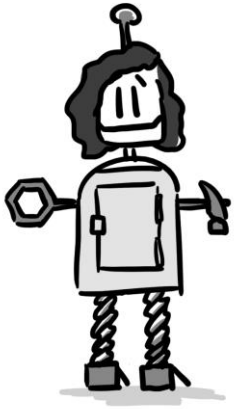

NO WAY!
OPINIONS
ISP / IT
Non-IT / Gov
Software or hardware being **certified** means it is secure.
They taught me how to take care of misconfigured systems **in school**.
Agility is more important than security.
In my company we have a **budget** for mistakes.
I trust all the **tools** and equipment we're using.
Too many things are **configurable**.
In my company we keep up with **security standards**.
My direct **supervisor** knows the amount of work I'm doing.
The obligation to **report** security incidents is often not taken serious.
Operators in management allow for more reasonable security-related business decisions.
My direct **supervisor** understands what I'm actually doing.
The general **priority** of security rises after a security incident has happened.
The threat of **bad press** after a security incident is what companies fear most.
The discovery of a security misconfiguration made me more **cautious** regarding security.
Blameless postmortems help to detect essential issues in corporate procedures.
I feel responsible for pointing out security issues to **peers**.
I feel **responsible** for keeping my operations secure.
ABSOLUTELY!
-2
-1,5
-1
-0,5
0
0,5
1
1,5
2

A few ideas

Wait for it… Waaait for it…

A few ideas

1. Automation.



A few ideas

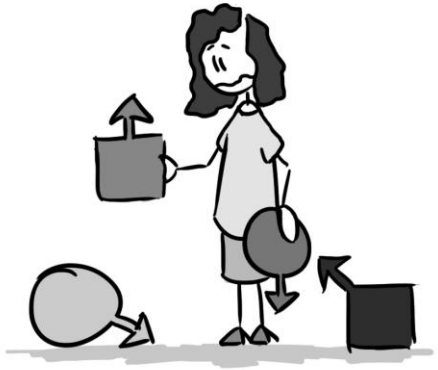
1. Automation.
2. Documentation.

A few ideas

1. Automation.
2. Documentation.
3. Clear (shared) responsibilities.

A few ideas

1. Automation.
2. Documentation.
3. Clear (shared) responsibilities.
4. Processes and procedures.



A few ideas

5. Troubleshooting courses for evolving operators.

“[In school] They only focus on installing and putting things together. Unless you learn to become a car mechanic or so. Where broken is the state you start with.”

− interviewee #11

A few ideas

6. Security incident “LARP” for management.

“Personally, I think some of them [the management] should use type writers instead of computers.”

− respondent #54

A few ideas

7. Probability. Damage. Human Factors.

“Usually it’s a question of whether the risk assessment was correct or needs adjustment, and following that sometimes security measures are enhanced.”

− respondent #52

A few ideas

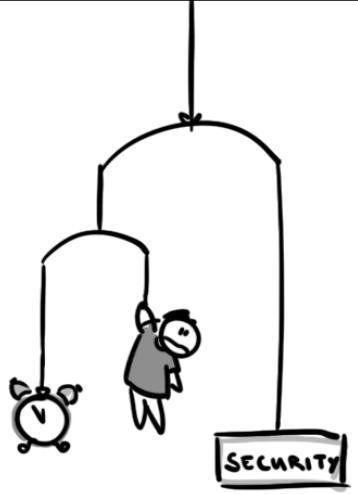
8. Honest error culture in companies.

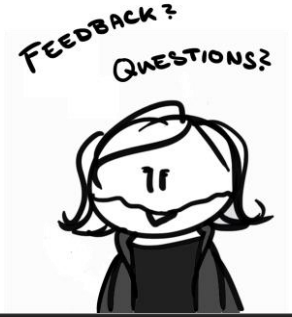
“A slap on the hand and off you go.”

– respondent #210

CONSTANZE DIETRICH
LEXTA Consultants Group

[@WeddingTrash // constanze.dietrich@lexta.com]





77th RIPE Meeting, Plenary Session, 16 October 2018

The Human Factors of Security Misconfigurations

Let’s Fix the Weakest Link.

A few ideas

1. Automation.
2. Documentation.
3. Clear responsibilities.
4. Processes and procedures.
5. Troubleshooting courses for evolving operators.
6. Security incident “fire drills” for management.
7. Probability. Damage. Human Factor.
8. Honest error culture in companies.