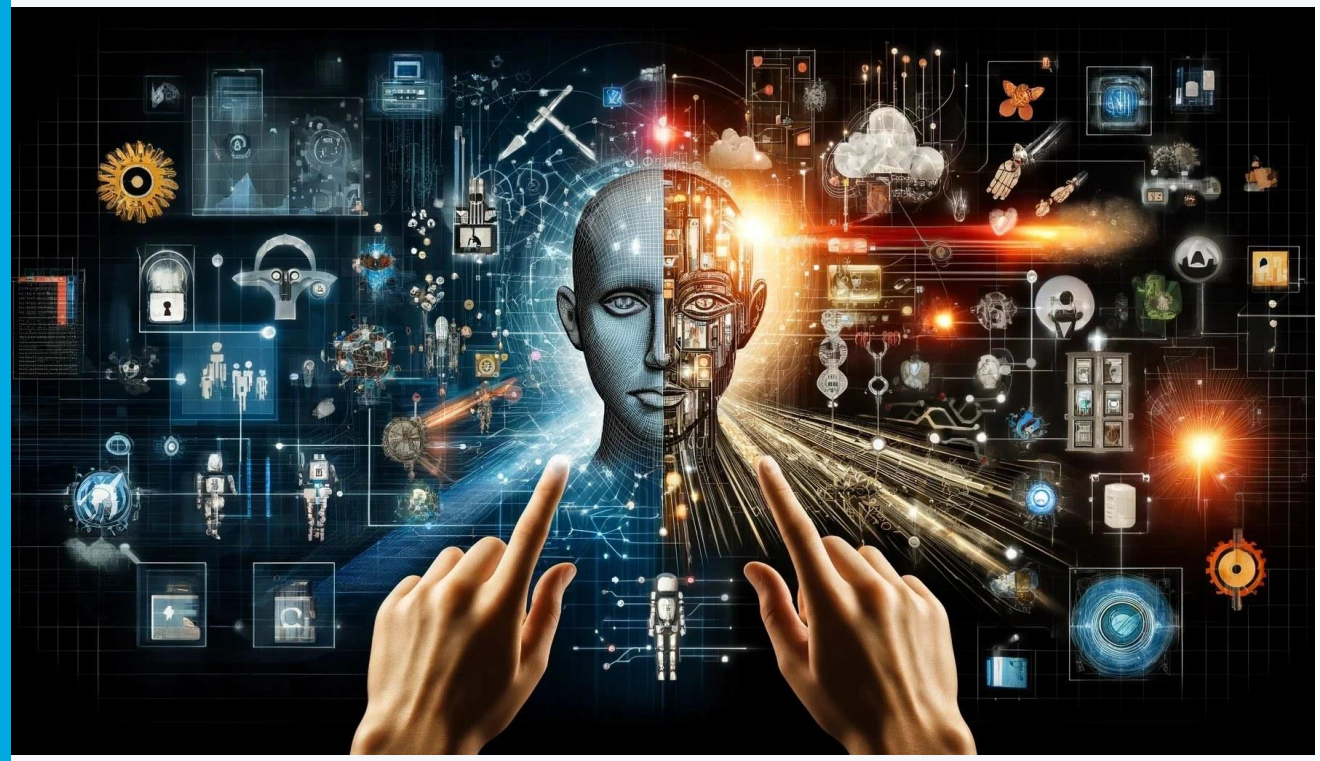
ISACA

ISACA Webinar

The Psychology Behind Cybersecurity

Why human behavior makes the difference



Nathalie Claes

2026

How long does it take before a hacker breaches your company?

74%

of all data breaches involve a human element

(Verizon DBIR, 2023)

Technology won't protect you if people leave the door open.

Your Speaker

Nathalie Claes

CISO Expert, author and keynote speaker with 20+ years in information security. Author of Hacked, Now What? (Pelckmans Publishers).

Credentials

Certified CISO, CISSP, ISO 27001/27701, DPO, Master IT Management

Regulatory Practice

NIS2 and DORA implementor for boards and security teams

Point of View

Security starts with people, not the firewall.

The human factor sits at the centre of every security decision.



Today's Session

What We Will Cover

Sixty minutes on the human side of information security, from bias to boardroom.

01	How Our Brain Deceives Us	Optimism, normalcy and authority bias, and why rational rules lose under pressure.	Psychology
02	Why We Click	Urgency, authority and reciprocity: the three instincts every phishing email exploits.	Social engineering
03	You Are the Target	Whaling, CEO fraud and BEC, with the FACC AG and Toyota Boshoku case files.	Cases
04	Training That Sticks	Simulations, five-minute monthly refreshers and reporting without punishment.	Awareness
05	Leadership as the Lever	Visibility, role modelling, psychological safety and five actions for tomorrow.	Culture



The Central Tension

Technology is the fence. The human is the open gate.

The Evidence

The Human Element Decides

74%

Breaches Involve People

Verizon DBIR 2023: 74% of breaches trace back to a human decision.

3

Instincts Attackers Exploit

Urgency, authority and reciprocity turn routine email into a way in.

— Controls hold the perimeter; judgement under pressure decides whether the door opens.

The Psychology

Four biases that betray us

Automatic thought patterns that quietly override objective security decisions



Optimism Bias

"That won't happen to me" — "IT handles that, right?"



Normalcy Bias

"Everything is probably fine." Suspicious email? Just spam.



Authority Bias

"The CEO is asking, so I'll do it" — even when the CEO is fake.

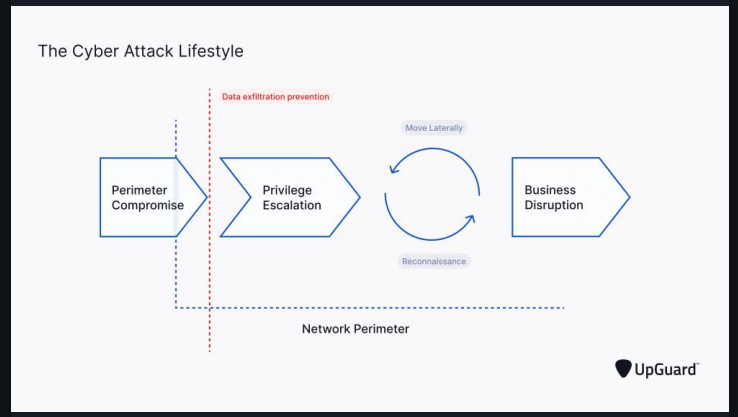


Confirmation Bias

"We're not an attractive target" — so warnings go unread.

Biases are automatic: security programmes cannot assume people will act rationally.

Why Do We Click?



3

Instincts phishing exploits: urgency, authority, reciprocity

Urgency

"Act now, your account will be blocked" forces a decision before thinking.

Authority

"Message from your bank or CEO" dresses a fake request as legitimate.

Reciprocity: a free gift, favour or helpful file creates the urge to give something back.

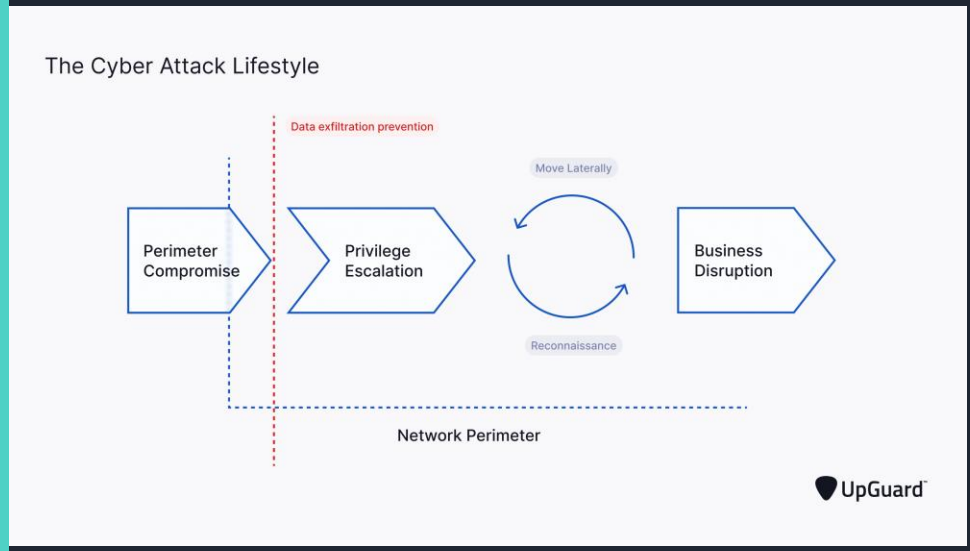
01

Signature authority · Public calendar

Why Attackers Study You

Your Habits Are Their Research Material

Travel dates, assistants and approval limits are public or guessable — the con is scripted before contact.



Case Files

One Email, One Click, Millions Gone

FACC AG

€50M

Austria, 2016 — whaling / CEO fraud

Attack type	**Whaling**
Pretext	**Secret buy**
Who acted	**The CFO**
Aftermath	**CEO & CFO fired**

Toyota Boshoku

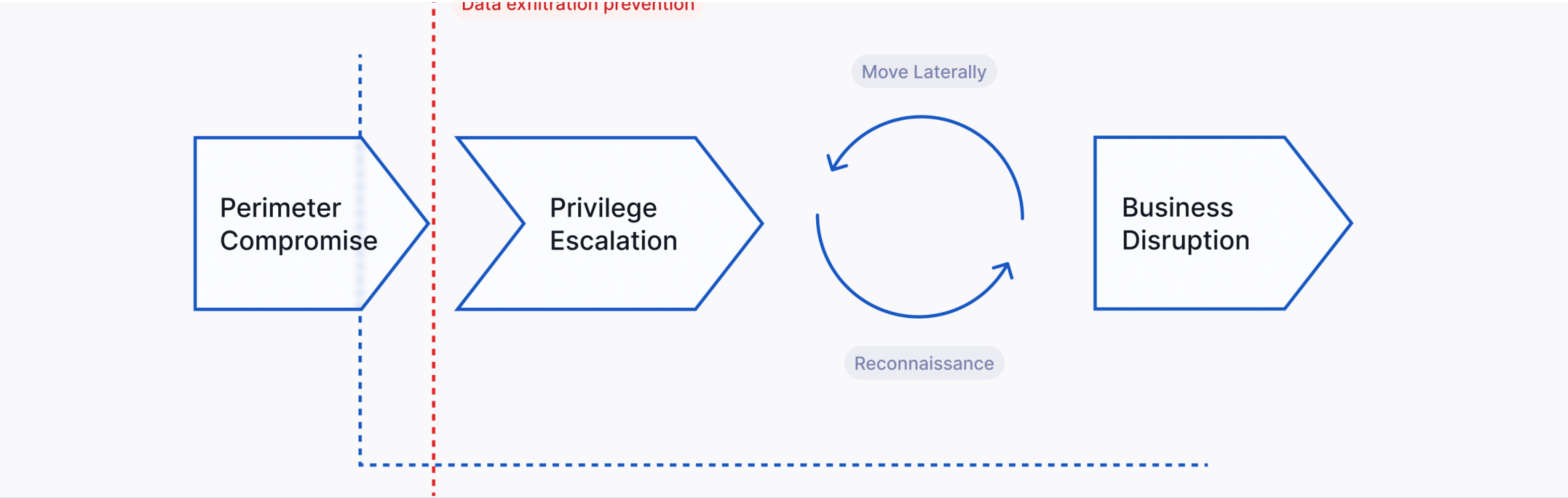
$37M

Japan, 2019 — business email compromise

Attack type	**BEC**
Pretext	**Urgent supplier**
Who acted	**Finance staff**
Trigger	**CEO instruction**

Authority bias plus urgency is the fatal combination behind both losses.

BEC Costs Billions — and NIS2 Makes It Personal



€2.7B

Annual worldwide damage from Business Email Compromise (FBI)

#1

Whaling: targeted phishing aimed at C-level executives

NIS2

CEOs are personally and legally responsible for cybersecurity

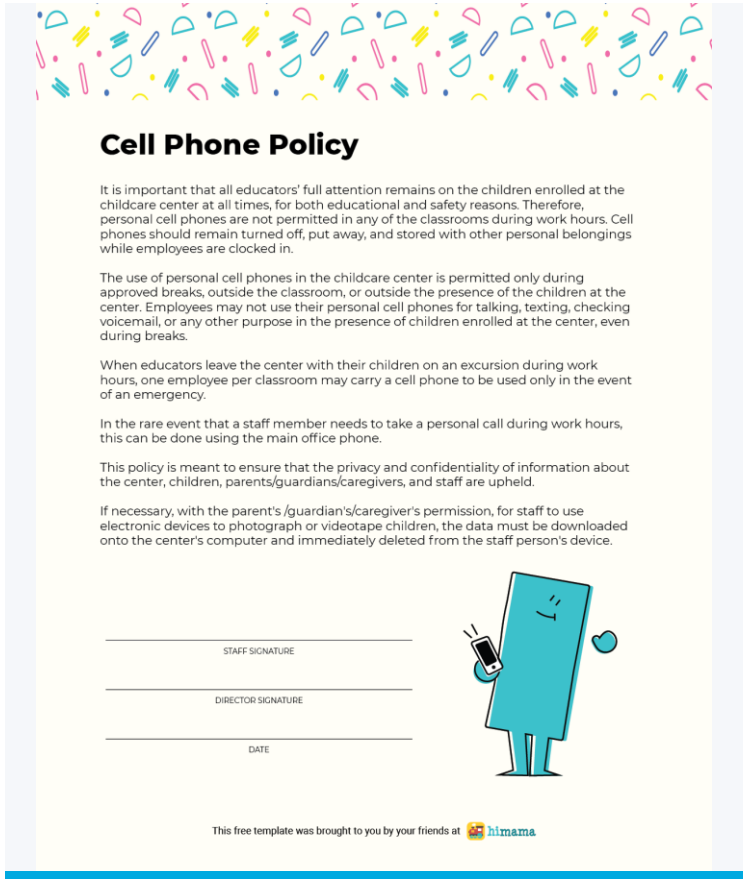
Training That Actually Sticks

One-time training fails — people forget and fall back into old habits.



Simulate

Run a phishing simulation — test the org, never punish clickers.



Cell Phone Policy

It is important that all educators' full attention remains on the children enrolled at the childcare center at all times, for both educational and safety reasons. Therefore, personal cell phones are not permitted in any of the classrooms during work hours. Cell phones should remain turned off, put away, and stored with other personal belongings while employees are clocked in.

The use of personal cell phones in the childcare center is permitted only during approved breaks, outside the classroom, or outside the presence of the children at the center. Employees may not use their personal cell phones for talking, texting, checking voicemail, or any other purpose in the presence of children enrolled at the center, even during breaks.

When educators leave the center with their children on an excursion during work hours, one employee per classroom may carry a cell phone to be used only in the event of an emergency.

In the rare event that a staff member needs to take a personal call during work hours, this can be done using the main office phone.

This policy is meant to ensure that the privacy and confidentiality of information about the center, children, parents/guardians/caregivers, and staff are upheld.

If necessary, with the parent's /guardian's/caregiver's permission, for staff to use electronic devices to photograph or videotape children, the data must be downloaded onto the center's computer and immediately deleted from the staff person's device.

STAFF SIGNATURE

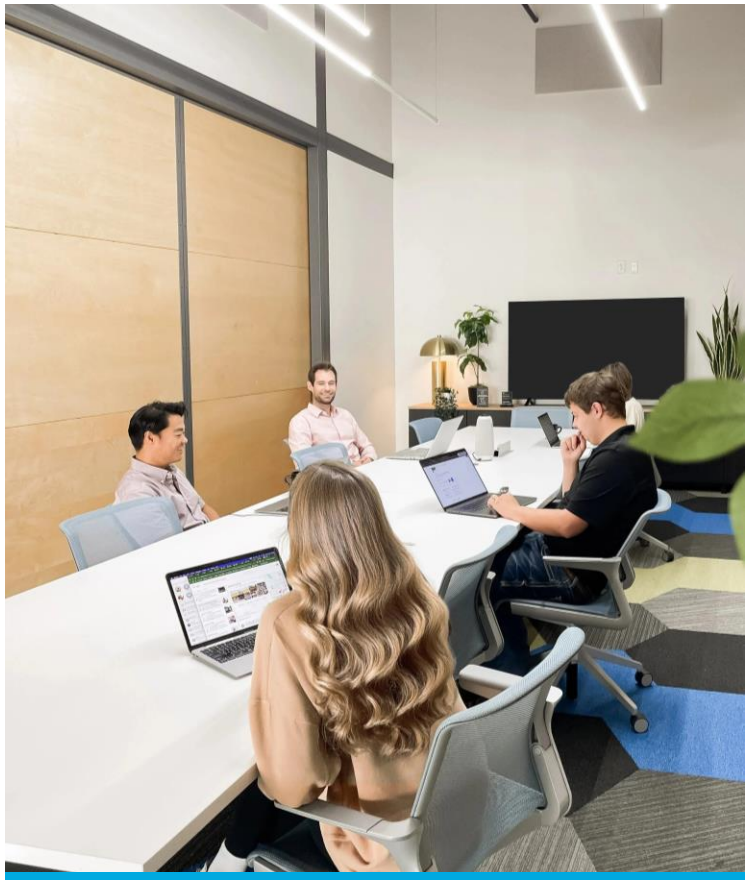
DIRECTOR SIGNATURE

DATE

This free template was brought to you by your friends at himama

Repeat

Five minutes of micro-training a month beats one annual session.



Reward

Reward reports of suspicious email; give one clear reporting channel.

Action Plan

Five Actions for Tomorrow

Each one has an immediate next step you can set in motion this week.

01 **Payment Verification Protocol** — Verify large payments by phone on a known number — never the one in the email.

02 **Simulate a Phishing Attack** — Schedule a simulation; never punish — use results as the training baseline.

03 **Regular Micro-Trainings** — Five minutes per month beats one annual session. Set a recurring monthly reminder.

04 **Nudging: Make Secure Easy** — Strong passwords by default, automated reminders, MFA mandatory from C-level.

05 **Reward Secure Behaviour** — Reward reporting of suspicious emails, punish no mistakes, publicise the channel.



Leadership

You Are the Greatest Lever

A security culture starts at the top. What you do, your organisation does — behaviour is modelled on what leaders practise, not on what policy states.

Visibility

Discuss cybersecurity openly in meetings and comms.

Role Modelling

Follow the rules too: MFA, strong passwords, no exceptions.

Psychological Safety

People must report mistakes without fear of punishment.

"Security is not an IT problem. It's a leadership problem."

Summary

Five Insights to Take Home

What this session argues, in five lines you can repeat to your board tomorrow.



Human Cause Dominates

Breaches have a human cause — technology alone is not enough.



Biases Spare No One

Optimism and authority bias make everyone vulnerable.



Executives Are Target #1

CEOs, not IT, are the primary target of whaling and BEC fraud.



Five Concrete Actions

Verification protocol, simulations, trainings, nudging, rewards.



You Are the Lever

Security culture starts at the top: what you do, the firm does.

— Security is not an IT problem — it is a leadership problem.

What Will You Do
Differently Tomorrow?

One decision can be the difference between a breach and a culture of security.

Set a Verification Protocol

Fix a payment threshold this week; verify every payment above it by phone on a known number, never the one in the email.

Make MFA Mandatory

Activate MFA for C-level first, then everyone. Strong passwords by default and automated reminders make the safe path the easy path.

Build a Reporting Culture

Communicate an internal reporting channel, reward reports of suspicious emails, and never punish the mistake.

Security Starts With People

Change starts with leaders: security is not an IT problem, it's a leadership problem. What you do, your organisation does.

Thank you

Questions? I'm here for you.

Email

nathalie@dadir.be

LinkedIn

linkedin.com/in/nathalieclaes

Website

www.dadir.be

'Hacked, Now What?'
Pelckmans Publishers



Security starts with people. Change starts with leaders.