Why we're not paying enough attention to security

Coenie Vermaak

Chief Technology Officer
Britehouse Automotive

dimension data | Let's do more.

What are the problems

Awareness

Comprehension

Misconceptions

Complacency

Common misconceptions

Cyber attacks orchestrated by "**Some dude in a basement**"

- Untrained
- Isolated
- Clad in a black hoodie & knows about Kali Linux

We're secure because we're behind a firewall

- Firewalls are misunderstood – they are just one layer of defense
- Filter based on IP addresses and port information – no broader context
- No consideration for payload content making it susceptible for spoofing
- Rules can become outdated or unnecessary potentially broadening attack surface

Cyber security is solely the responsibility of the IT department

- Developers must work closely with security professionals to implement strategies against malicious actors
- Problem-Solving and proactive threat mitigation are integral parts of software development
- Everyone interacts with systems, data and devices daily

Misunderstanding of modern cyber adversaries leads to complacency in security measures

Professional organized crime

- Hackers and organized crime groups are becoming increasingly sophisticated
- Organized crime groups implement incentives and bonus structures
- Have budgets that rival that of major global corporations
- Collaboration and specialization contribute to growing criminal economy
- Complex global networks with crimes spanning cross-country borders

72% increase in data breaches in 2023 compared to previous high in 2022

(Cybersecurity Ventures)

2023 - Globally 72.7% of all organizations was impacted by ransomware attacks

(± 333 Million Organizations)

Estimated $ 10.5 trillion worldwide cost associated with cybercrime in 2025

(Forbes)

Global average cost of a data breach in 2023 was $ 4.45 million

(IBM)

What is the significance of Cyber Security in our daily lives

- Safeguarding sensitive data from unauthorized access
- Protecting privacy to preserve our identities
- Preventing financial loss
- Ensuring (business) continuity
- Maintaining Normality

Some common daily threats

Malware

Phishing

Spoofing

Password Attacks

Denial-of-Service

Crypto-jacking

Financial Implications

Cyber Criminals and Syndicates

- Lucrative business within an ever-expanding market
- Opportunities for basement-hacker and government sponsored syndicates
- Business focus tend to be on prevention and remediation and not prosecution or threat elimination

Curbing the reward and raising the risk could lead to a decreased cadence

Businesses and Overall economy

- Suffer substantial direct financial losses due to cyber attacks
- Incidents disrupt normal business operations leading to additional costs
- Reputational damage
- Legal and regulatory costs
- Increased cyber security spending

Human behaviors contributing to security vulnerabilities

Negligence & Error	Rushed work, distractions and lack of awareness
Emotional Responses	Human traits like helpfulness, curiosity and naivety
Password Hygiene	Weak, reused passwords often stored insecurely
Denial	Assumptions lead to denial of risk & responsibility
Convenience	Irresponsible usage of public Wi-Fi networks
Over Share	Personal details on social media
Social Conformity	Social norms influencing how people behave
Learning & Adaptation	Humans learn from experiences and adjust behavior

State of security awareness and threat landscape

The Law of accelerating returns, which states that technology speeds up over time because there is a common force driving it forward, also apply to Cyber crime

The more successful the endeavor, the greater the adoption and attention it receives

- Cyber attacks are on the rise
- Will include more sophisticated AI techniques such as advanced phishing and deepfakes
- Attack surface ever expanding

- Move away from traditional architectures towards Zero trust architectures
- Greater threat intelligence sharing
- Focused user training and awareness
- Incident response plans

Real-World Example

2020 – Data breach at a credit bureau

Deemed insignificant: some names and email addresses exfiltrated

2024 – Data breach on messaging platform

Deemed insignificant: some names and email addresses exfiltrated

1 Long term impact of security incidents

2 Sophistication of cyber crime syndicates

3 Capabilities and orchestration when enriching data sets

4 Vulnerability of people to unwittingly participate

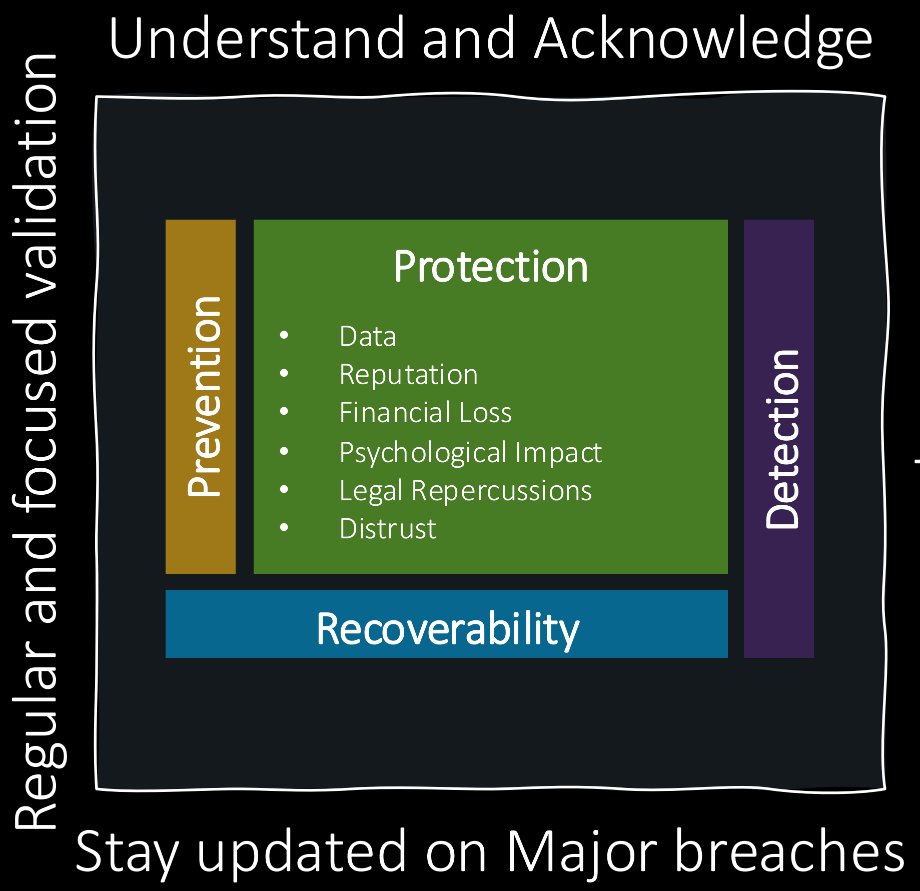
5 Requirement to continuously focus on and adapt protocols

6 Importance of securing data and environments

2024 – Significant Data breach at an insurance company

Data from previous breaches (and some data scraping techniques) used to bypass identification and verification screening leading to the exfiltration of Names, residential addresses, identity numbers, cellphone numbers and details of items covered by policies

What can we do



Understand and Acknowledge

Regular and focused validation

Continual improvement

Prevention

Protection

- Data
- Reputation
- Financial Loss
- Psychological Impact
- Legal Repercussions
- Distrust

Detection

Recoverability

Stay updated on Major breaches

Improve security posture by implementing robust security strategy

Prevention

- Application Security – adding security features to prevent cyber attacks that exploit vulnerabilities in the source code
- Education – Empower people to understand and mitigate threats

Protection

- Network Security – measures include firewalls, intrusion detection, encryption and ensuring confidentiality during transmission
- Operational Security – policies, procedures and practices to protect operations
- End-User Security – Password hygiene, responsible use of technology, etc.
- Data Encryption – encrypt sensitive data at rest

Detection

- Threat Intelligence – compares signature data from known attacks
- Network traffic analysis - detect anomalies or suspicious behavior
- Deception technology – protects against threats from attackers that infiltrated network, it sets traps and decoys to mislead attackers and detect their presence

Recoverability

- Disaster Recovery planning – steps to restore systems, data and operations after a cyber incident

Protect data and systems

Confidentiality

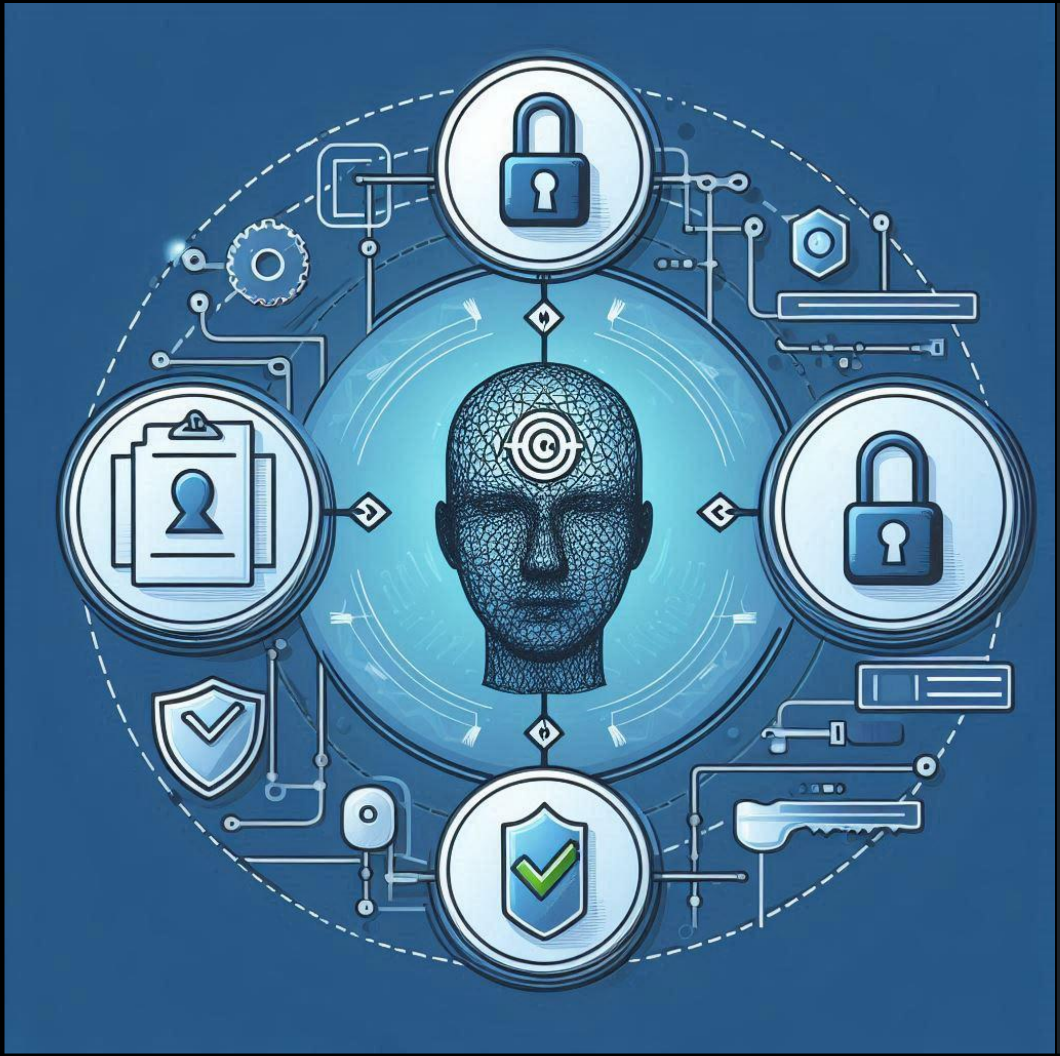
- Ensure data is hidden; Only visible to and accessible by Authorized users
- Enforced through – Encryption

Integrity

- Accuracy and completeness of data, assurance that data has not been modified or omitted
- Enforced through – Hashes

Availability

- Data is available when required
- Enforced through – Redundancy



Identity and Access Management

Identification

- Process of identifying an entity
- Possible to identify without authenticating
- Essentially a claim

Authentication

- Can only be done after identification
- Password, PIN, Biometric
- Implement principle of non-repudiation – cannot claim that the authenticated entity did not perform the action
- Authenticate with something that the entity Knows, Owns, Is

Authorization

- Set Access Control Limits
- Always apply minimum privileges that is required
- Beware of privilege creep

Accountability

- Account Audits & Log Reviews

Security best practices

Update and enforce security policies

- Don't become complacent
- Consider Risk, Legal and Regulatory concerns
- Secure software development framework – NIST National Institute of Standards and Technology (nist.gov)

Treat Security as a Priority

- Implement a robust security strategy
- Install security updates and backup data
- Require the use of strong passwords and multi-factor authentication
- Patch Management
- Employee Training

Include security measures in SDLC - Automate Processes

- Code Reviews
- Vulnerability scans

Threat Modeling

- Analyze software architecture to identify vulnerabilities
- Design with security in mind

Tools and Technology

Encryption Overview and Usage

Symmetric Encryption – Private key encryption

- The same key is used for encryption and decryption
- Same cipher used for encryption and decryption
- Key length determines the strength of the encryption
- Require secure mechanism to share key – interception remains concern

Asymmetric Encryption – Public key encryption

- Public key of destination used to encrypt; decrypt using destination private key
- Public key cannot be used to decrypt content
- Digital signatures can be created by encrypting content with private key and decrypting with public key – this is used for authenticity, not security
- Slower than Symmetric encryption

Hashing

- One-Way encoding – impossible to recover original
- Should be unique – different inputs must lead to different hashes
- Major use-case is for verifying file integrity

OpenEdge TDE

Purpose

Transparent Data Encryption protects data stored on disk - focusing on data-at-rest security, unlike network encryption that focus on security during transmission

Core Functionality

Database Master Key

- Each encrypted database has a unique DMK
- Managed by Administrator
- Stored separate from database

Encryption Policies

- Defines which database objects are encrypted
- Specify the encryption cipher

Transparent Decryption

- Encryption / Decryption process transparent to connected clients

Hardware Security Model (HSM) Support

Purpose

Provides a secure environment for cryptographic operations, facilitating the protection of sensitive data and supporting compliance

Core Functionality

Temper resistant hardware – Ensuring integrity of Keys

Authorized access – Makes keys available only to authorized users

Enhanced security – No need to load key into server memory

OpenSSL 3.1 & TLS 1.3 Support

Purpose

OpenSSL 3.1 is the latest version of the open-source cryptographic library. It's a full featured toolkit for general-purpose cryptography and secure communication.

Core Functionality

Enhanced Security

- TLS 1.3 improves security protocols and cryptographic algorithms
- Promotes robust encryption for OpenEdge applications

Provider-based approach

- OpenSSL 3.1 introduce concept of Providers
- Providers collect various algorithms ensuring the latest and strongest cryptographic options
- OpenEdge currently use Default and Legacy Algorithms
- Legacy provider won't be supported in future releases – best to use algorithms from default provider

Code Signing

Purpose

OpenEdge 12.8 – Application code can be digitally signed to facilitate application integrity and execution of trusted software

Core Functionality

Integrity Verification

- Ensure that code remains unchanged after it is signed
- Users can check integrity of code by checking digital signatures

Authenticity and Trust

- Signed code provides proof of authenticity
- Users can trust that the application [code] comes from a trusted source
- Reduces risk of running malicious or tampered code

Dynamic Data Masking (DDM)

Purpose

Conceal sensitive data at run-time to ensure compliance with regulations like GDPR or POPIA.

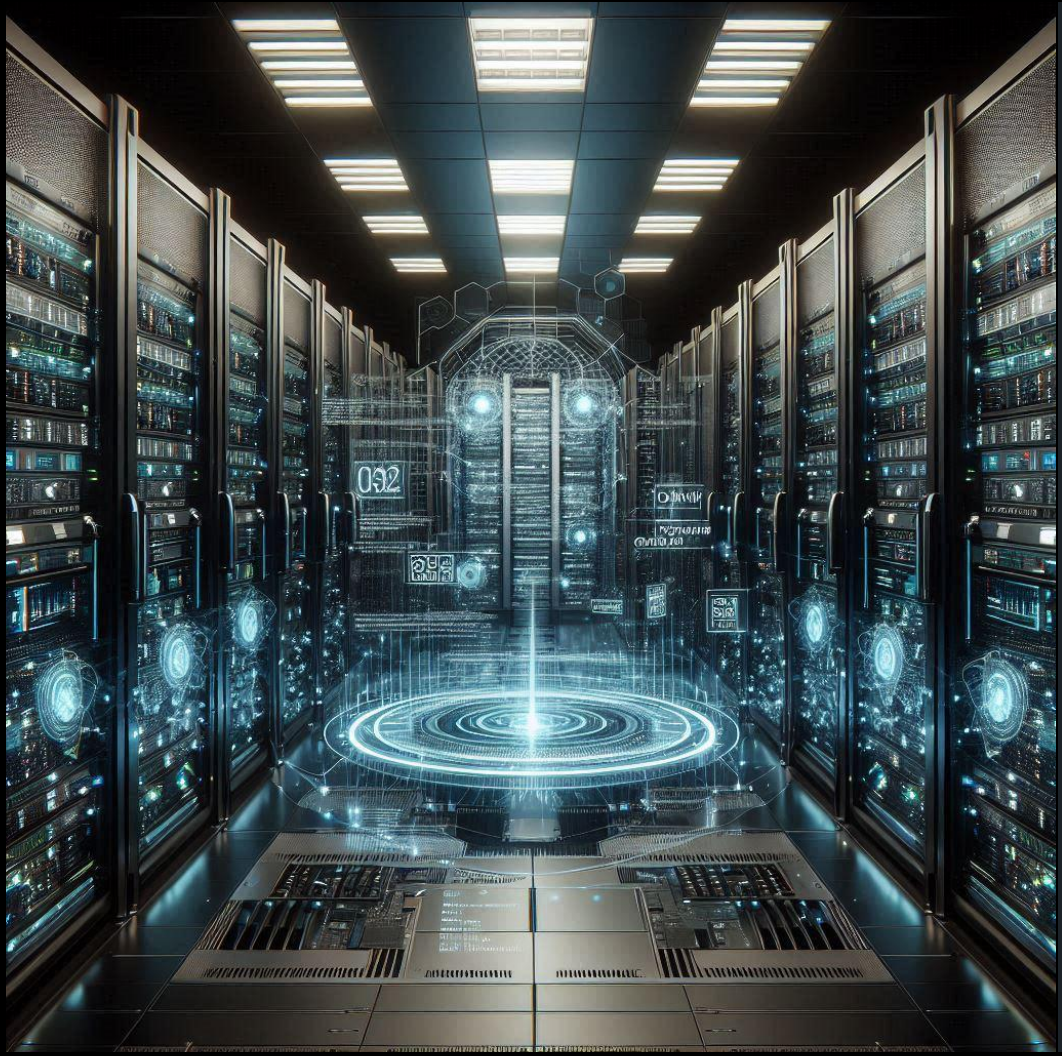
Core Functionality

Purpose and Benefits

- Control the amount of data exposed to different users and roles
- Hides sensitive data from view while underlying data remains unchanged
- Minimized risks related to unauthorized access and data breaches

Seamless integration

- No code changes required
- Use authorization tags and role settings to control data visibility
- Works across all clients



Enhanced Application Server

Purpose

Several improvements included in OE 12.8 to facilitate improved security, better control and productivity

Core Functionality

Security

- JWE Tokens now supported for enhanced enterprise security
- OAuth2 Token Authentication through OpenEdge Authentication Gateway

Productivity

- New and enhanced command-line utilities to streamline PASOE migration and management
- Improved Session lifecycle management

Incident Response Planning

Purpose

Crucial plan or set of written instructions that guide the response to a security incident. Detailed and well reasoned planning will minimize the impact and mitigate risks

Core Functionality

Components to consider

- **Recovery steps** – list of activities that outline the road to recovery
- **Roles & Responsibilities** – who does what during an incident

Plans to consider

- **Incident Response Plan** (IRP) – Address incidents without business interruption
- **Business Continuity Plan** (BCP) – Keeps operations running during disruption
- **Disaster Recovery Plan** (DRP) - Returns business to original state after incident

In Summary

- Fully appreciate the scale and implications of cyber crime
- Cyber crime is a lucrative enterprise and both the scale as well as the target landscape is constantly growing
- Consciously act against cyber crime by
  - Using strong and secure passwords
  - Keep cyber threats top of mind in all digital activities
  - Filter information that is shared
- Cyber security strategy should include the following elements
  - Prevention
  - Protection
  - Recoverability
  - Detection
- Consider security - include safeguards in all issues or designs you deal with
- Cyber incidents is not a matter of IF anymore, but a matter of WHEN

Questions