SecurityFirst

INTRODUCING SECURITYFIRST (METACOMPLIANCE)

Systems make life easy, they don't forget and they can be in more than one place at any time; a neat trick!

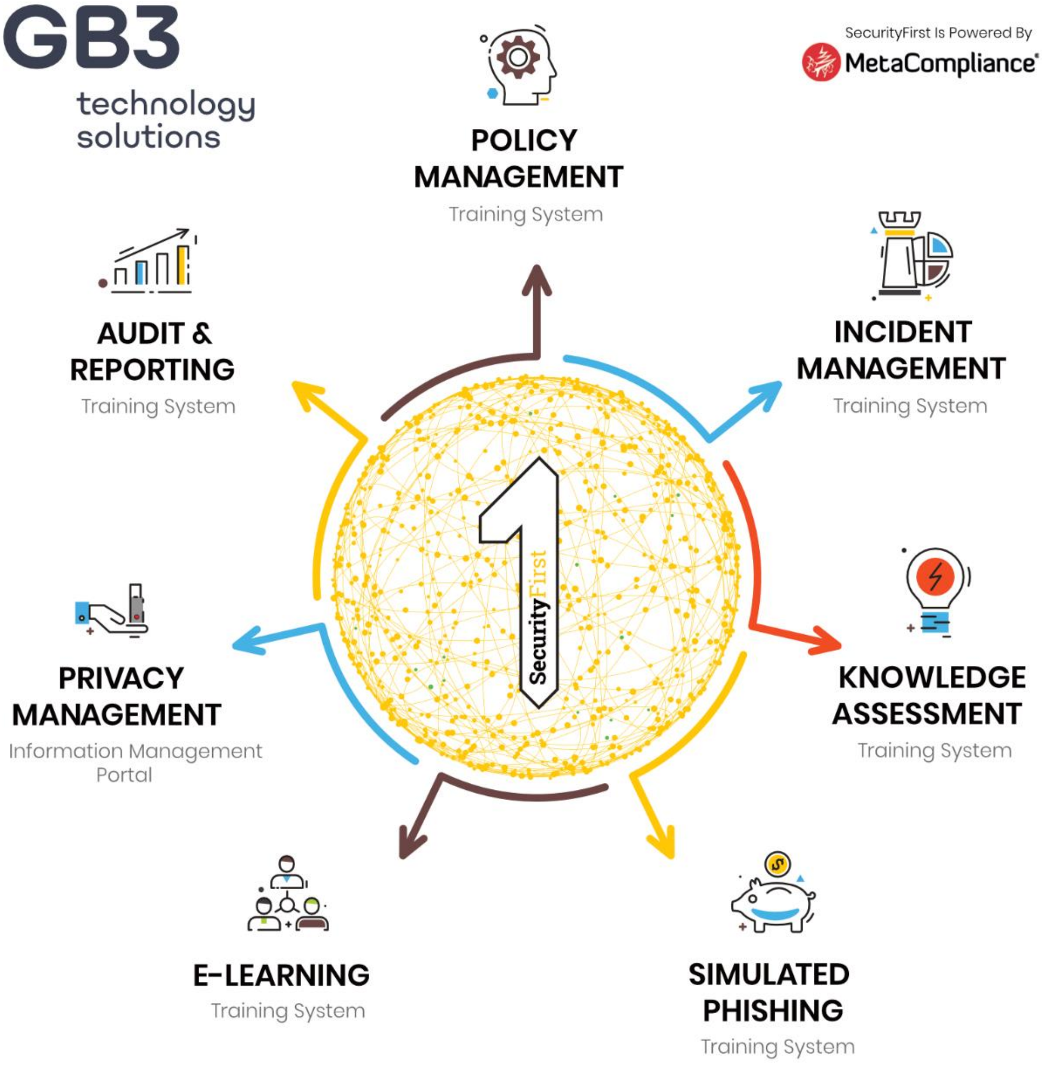
Talking of neat tricks, each Heading in this document will navigate you to the web page explaining the section in detail.

GB3 have partnered with MetaCompliance to provide the SecurityFirst offering. MetaCompliance hosts our training portal and GDPR management platform.

So why use GB3 rather than go direct to MetaCompliance? Firstly, you get to share our enterprise level volume discount and then you get to use our experts to implement and manage the system properly.

WHAT DOES IT INCLUDE?

Here's what's included in the SecurityFirst software: -



Protecting information is critical to your organisation

October 2020

eLearning (MetaLearning)

What is it?

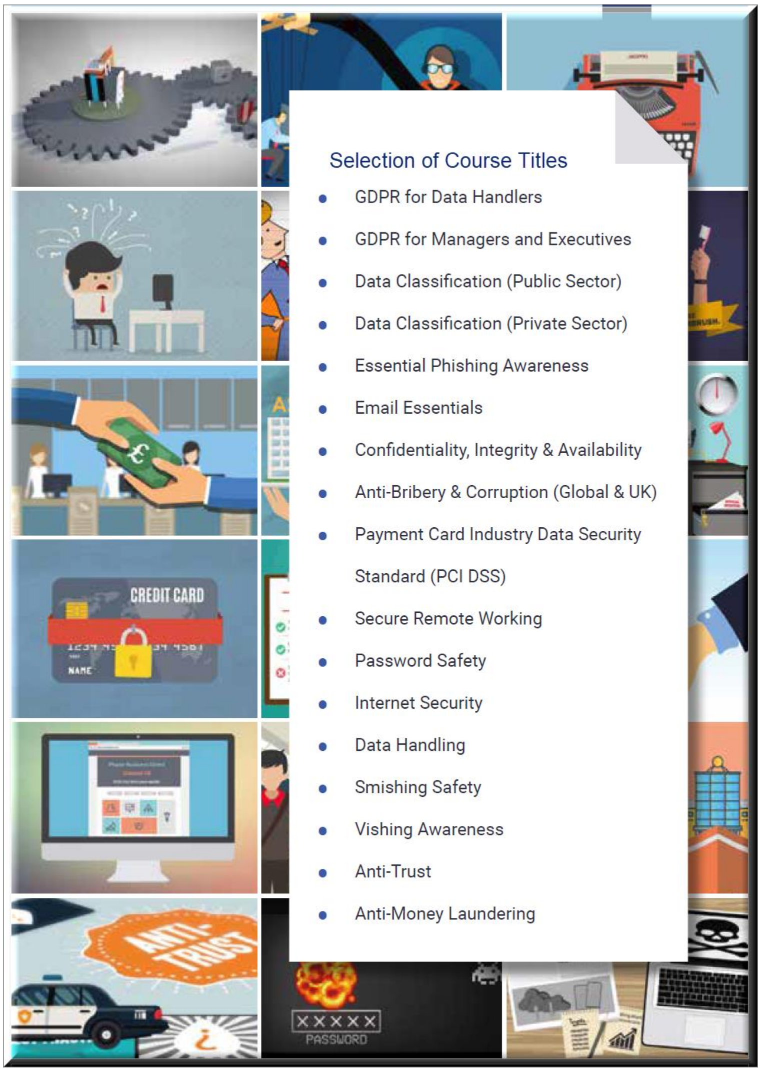
MetaLearning is best practice information security, data protection and compliance eLearning.

The high-quality MetaLearning library is designed to engage users with graphically rich and interactive learning experiences.

Using stories, realistic scenarios and narratives for context, MetaLearning provides gamified eLearning services that are engaging and fun.

It consists of 2 types of Learning:

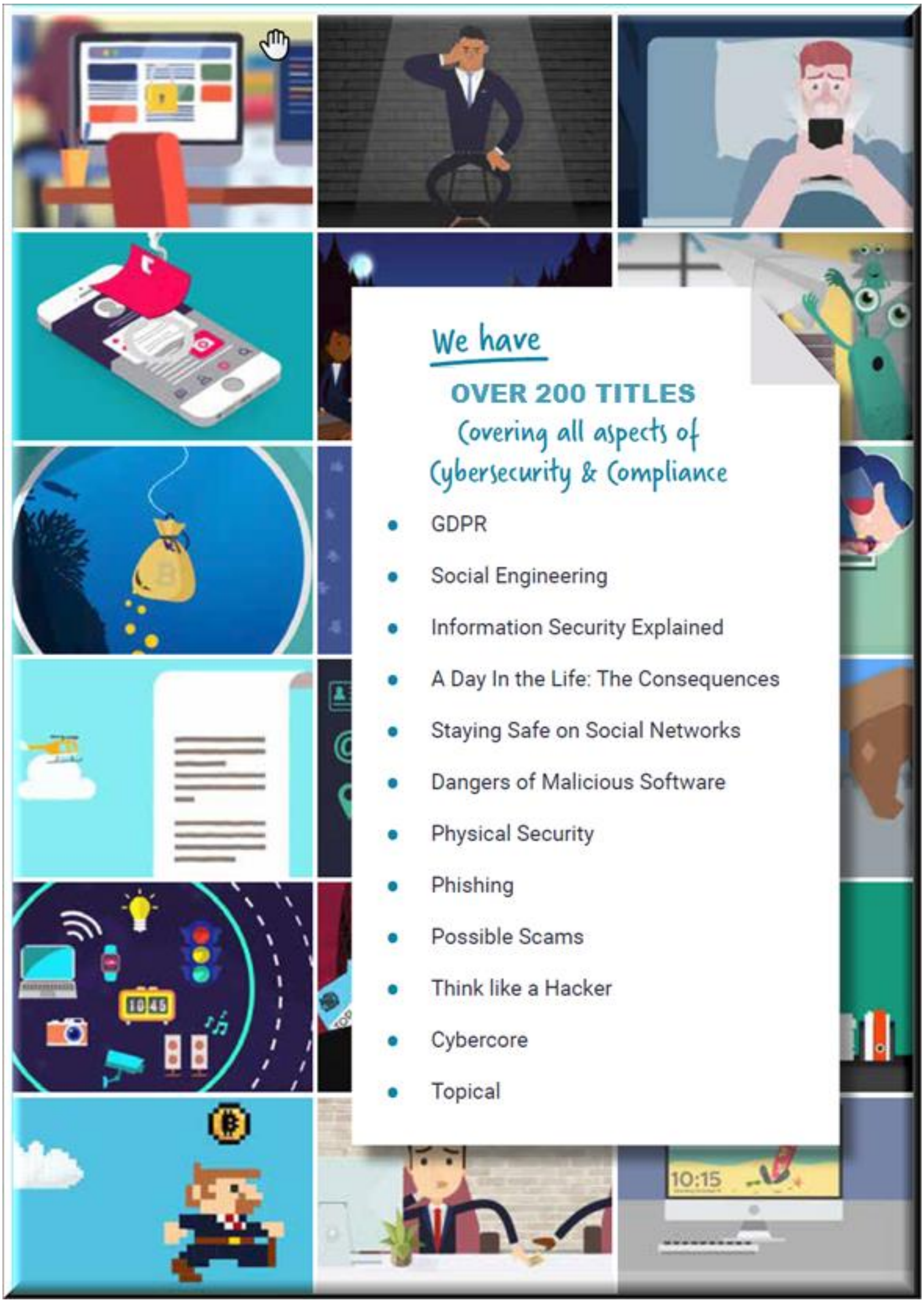
- Compliance – SCORM based learning modules with tests (Pass / Fail)
    - Currently 23 in total



Selection of Course Titles

- GDPR for Data Handlers
- GDPR for Managers and Executives
- Data Classification (Public Sector)
- Data Classification (Private Sector)
- Essential Phishing Awareness
- Email Essentials
- Confidentiality, Integrity & Availability
- Anti-Bribery & Corruption (Global & UK)
- Payment Card Industry Data Security Standard (PCI DSS)
- Secure Remote Working
- Password Safety
- Internet Security
- Data Handling
- Smishing Safety
- Vishing Awareness
- Anti-Trust
- Anti-Money Laundering

- Nano – Short educational videos, usually about 2-3 mins in duration
  - Currently there are over 270 in total



We have

OVER 200 TITLES

Covering all aspects of Cybersecurity & Compliance

- GDPR
- Social Engineering
- Information Security Explained
- A Day In the Life: The Consequences
- Staying Safe on Social Networks
- Dangers of Malicious Software
- Physical Security
- Phishing
- Possible Scams
- Think like a Hacker
- Cybercore
- Topical

GDPR Management (MetaPrivacy)

What is it?

The software provides an easy to follow workflow to guide specialist stakeholders through the review and approval phases of the lifecycle.

Privacy risks and any associated remediation tasks can then be created, assigned and tracked within the system.

In addition, MetaPrivacy© includes role-specific GDPR online learning modules, advanced policy management capabilities, step-by-step guidance for managing privacy incidents and a collection of informative dashboards and reports that allow you to monitor privacy compliance programs and demonstrate accountability as required.

Think MetaPrivacy
Think of a single place to record your
Data Processing Activities, Create Your Risk Register,
Manage Staff Policies, Train Users on GDPR and
Demonstrate GDPR Compliance.

PHISHING (METAPHISH)

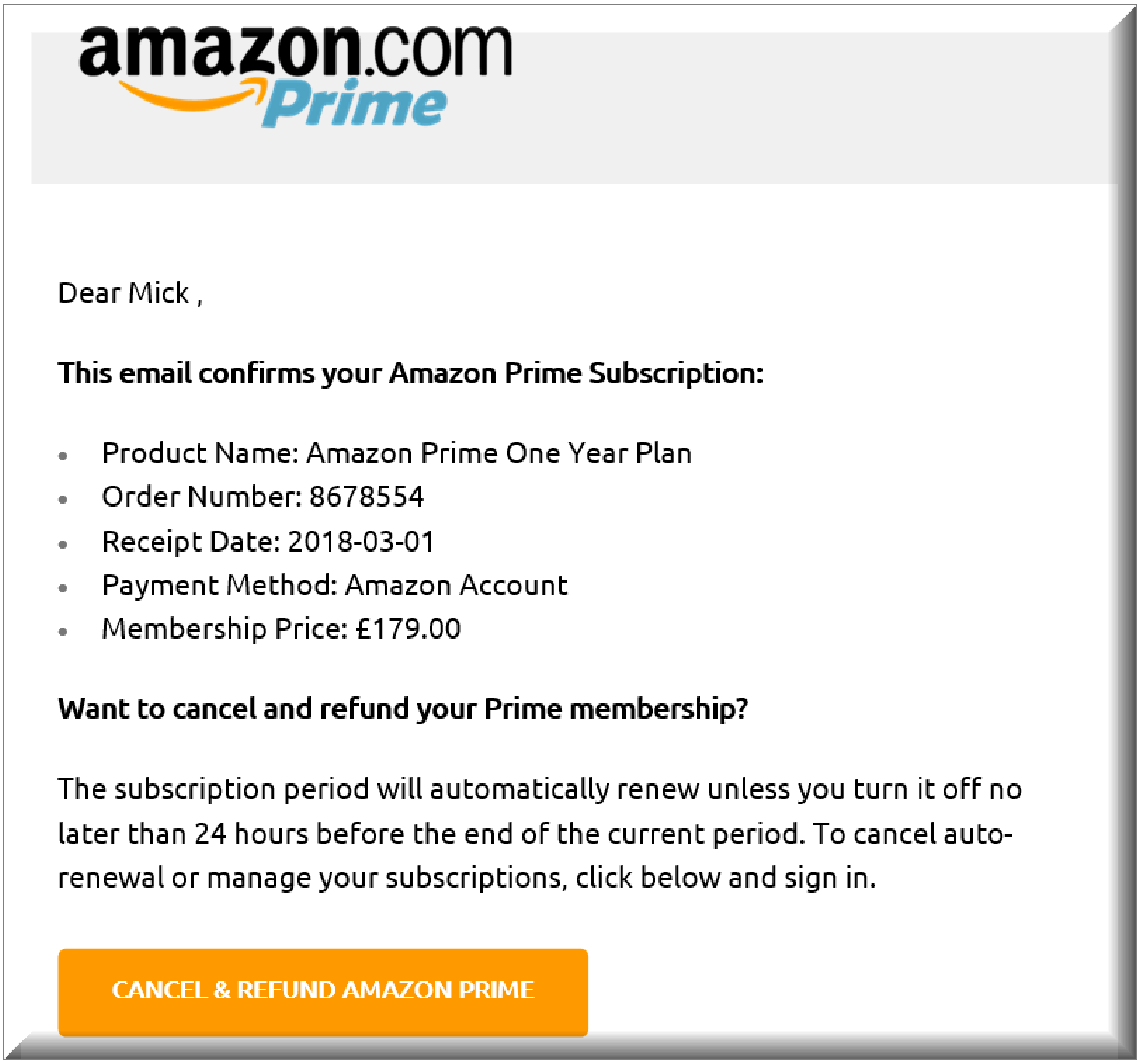
WHAT IS IT?

Phishing and Ransomware attacks are targeted directly to your staff and management.

MetaPhish increases your employees' sensitivity to these fraudulent emails.

This phishing simulation software provides you with the means to measure your current risk level from a phishing attack.

The user is also afforded the opportunity to work through a learning experience based on their failure to spot the phish.



Dear Mick ,

This email confirms your Amazon Prime Subscription:

- Product Name: Amazon Prime One Year Plan
- Order Number: 8678554
- Receipt Date: 2018-03-01
- Payment Method: Amazon Account
- Membership Price: £179.00

Want to cancel and refund your Prime membership?

The subscription period will automatically renew unless you turn it off no later than 24 hours before the end of the current period. To cancel auto-renewal or manage your subscriptions, click below and sign in.

Policy Management

What is it?

All information assurance frameworks such as ISO 27001 have information security policies as their basis.

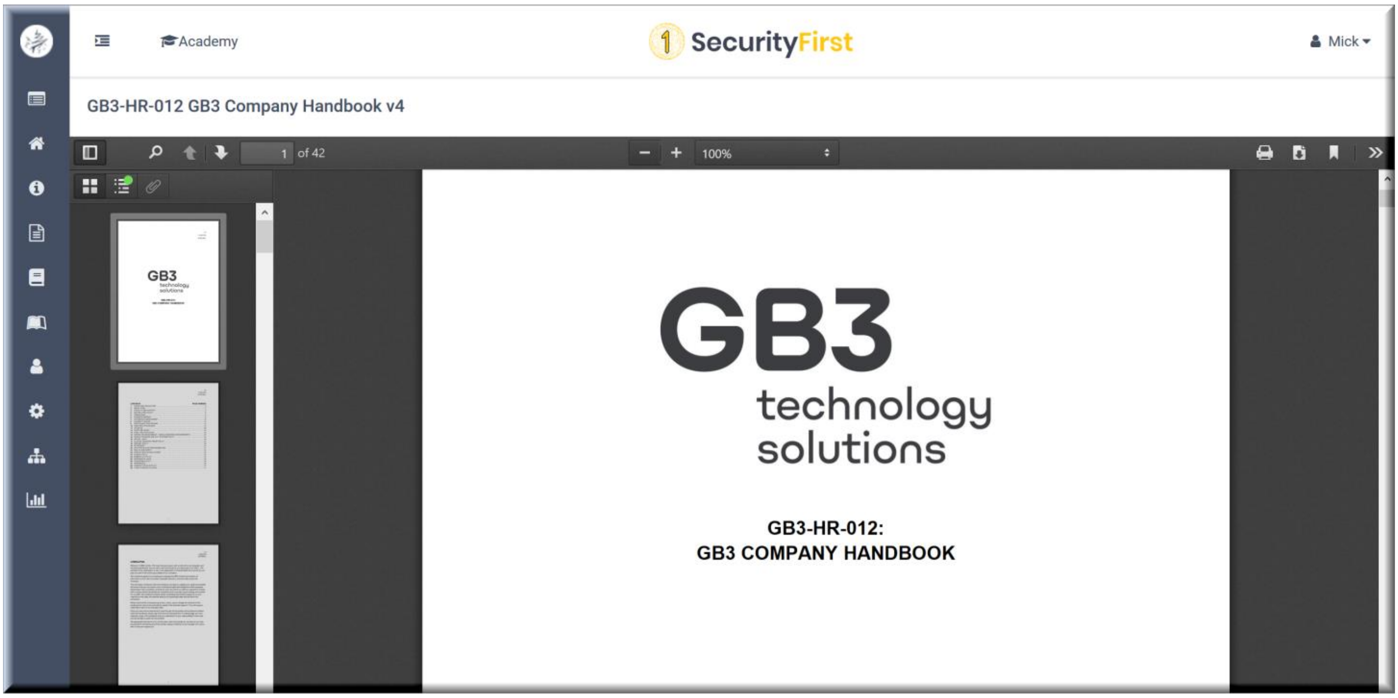
Similarly, all major regulatory oversight requirements begin with writing compliance policies.

These policies guide staff and partners on the relationship the organisation has with current legislation and industry regulations.

The MetaCompliance Policy Management software contains all the key elements required to automate, deliver and manage your organisation's policy management life cycle.

Key Features include:

- Consistent method of creating policies
- Tracking of attestation and responses from staff
- Determine employee understanding of the policy
- Target or exempt specific groups of users
- Obtain real time reporting and adoption of policies across the organisation
- Allow Third Parties to access corporate policies remotely
- Automate the policy approval process
- Ability to have Cloud Based or on-premise implementations of the software
- Easy to use administration interface



GB3-HR-012 GB3 Company Handbook v4

GB3 technology solutions

GB3-HR-012:
GB3 COMPANY HANDBOOK

INCIDENT MANAGEMENT (METAINCIDENT)

WHAT IS IT?

One of the signs of improving Information Security and compliance awareness will be increased vigilance of potential issues by your staff.

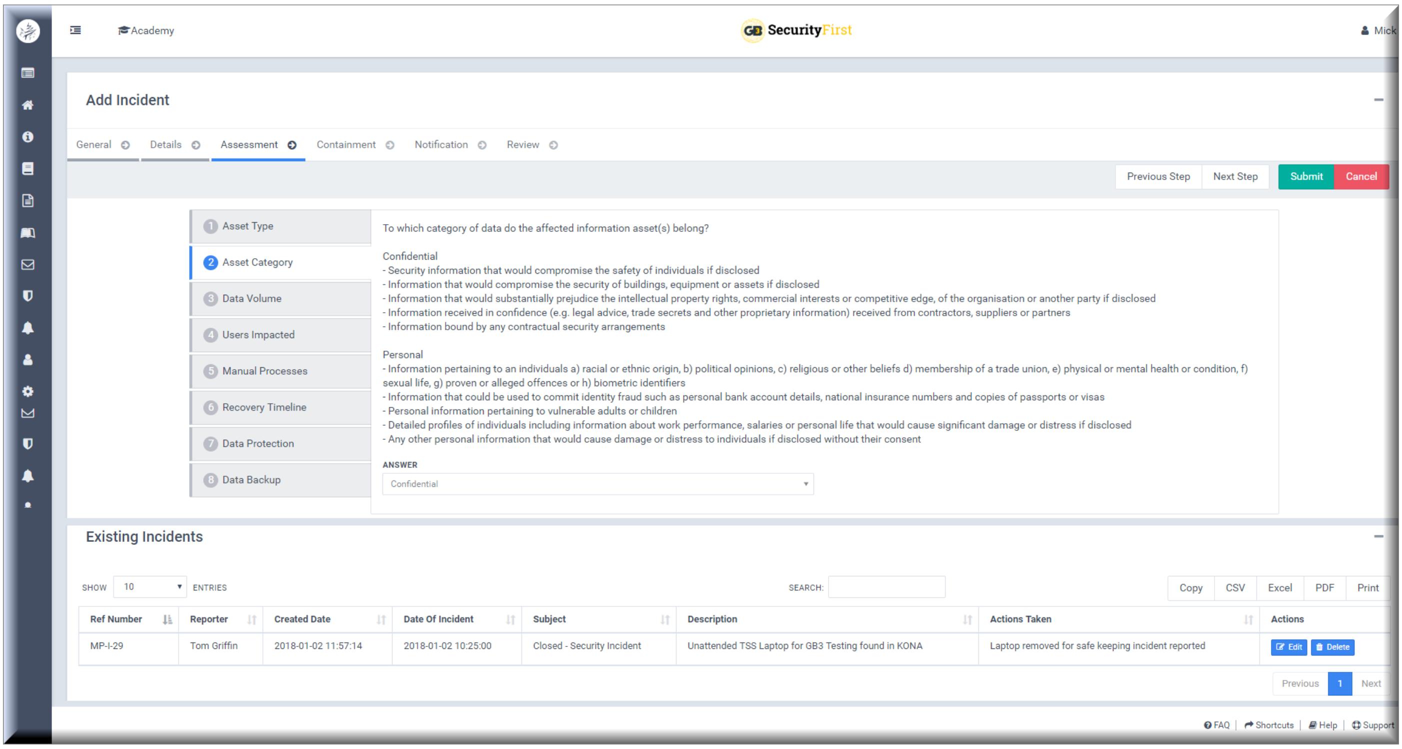
Being successful in improving the maturity of your Information Security and compliance posture means that there will be an increase in the number of incidents that staff will want to report.

The key is to ensure that you respond to these reported incidents in a timely manner.

It is imperative that staff have an easily accessible and simple method of reporting possible problems.

The incident management functionality with the MetaIncident module provides a lifecycle view of incident management and provides an incident register to manage issues.

The system provides necessary audits to report to regulators and governance committees.



Add Incident

To which category of data do the affected information asset(s) belong?

Confidential
- Security information that would compromise the safety of individuals if disclosed
- Information that would compromise the security of buildings, equipment or assets if disclosed
- Information that would substantially prejudice the intellectual property rights, commercial interests or competitive edge, of the organisation or another party if disclosed
- Information received in confidence (e.g. legal advice, trade secrets and other proprietary information) received from contractors, suppliers or partners
- Information bound by any contractual security arrangements

Personal
- Information pertaining to an individuals a) racial or ethnic origin, b) political opinions, c) religious or other beliefs d) membership of a trade union, e) physical or mental health or condition, f) sexual life, g) proven or alleged offences or h) biometric identifiers
- Information that could be used to commit identity fraud such as personal bank account details, national insurance numbers and copies of passports or visas
- Personal information pertaining to vulnerable adults or children
- Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress if disclosed
- Any other personal information that would cause damage or distress to individuals if disclosed without their consent

ANSWER: Confidential

Existing Incidents

SHOW 10 ENTRIES SEARCH:

Ref Number	Reporter	Created Date	Date Of Incident	Subject	Description	Actions Taken	Actions
MP-I-29	Tom Griffin	2018-01-02 11:57:14	2018-01-02 10:25:00	Closed - Security Incident	Unattended TSS Laptop for GB3 Testing found in KONA	Laptop removed for safe keeping incident reported	Edit Delete

GB3 Managed Service

(SecurityFirst)

GB3 will be responsible for the portal

- Customer would be Managed by GB3 (See Note 1)

Setup

- GB3 will commission the Tenant (Portal)
- GB3 will provide 1/2 day of consultancy, this would cover:
    - "Onboard" a designated administrator
        - Nominated Administrator account creation
        - System "Walkthrough"
        - Show in built User Guide
        - Show how to log support calls
        - Show how to run reports
    - Add all users to system
    - Add all available policies to Tenant (Portal)
        - This a "One time" task, additional uploads / changes will be managed by the administrator.

Managed Service over the year

- Deploy 1 course per month (1st course being "Phishing")
    - Subsequent courses identified in quarterly review (See Note 2)
- Two phishing assessments, 1st one being in month 2 following phishing course.
- A Webex meeting every quarter to discuss the next 3 months, ie what courses.
- Incident Management (See Note 3)
- Be available to assist with additional training, course creation, additional phishing assessments, policy management (See Note 4)

Note 1

The application allows for the administration of the portal to be handed over to the customer should it be required.

- Stage 1 – Month 3 – The ability to run the portal is given to the administrator, this allows course creation, phishing creation, policy management, incident management

Note 2

A detailed Course catalogue is attached showing both Compliance and Nano titles, new ones are being added all the time.

Note 3

Incident Management - these will be handled by the designated administrator once logged by a user.

Note 4

Additional support can be provided at an agreed cost

MetaPrivacy Module – The software comes with a Privacy module, this is included in the price but the following needs to be considered:

- All other modules are user friendly, however the Privacy Module is a detailed and complex module to initially set up.
- Once set up the module becomes as self-intuitive as all the other modules.
- It takes approx. 1 day of additional support from GB3 to deploy and train this module, this is not included in “Standard Managed Services”
- If GB3 are conducting your GDPR Implementation, the consultant will use MetaPrivacy on your behalf.

SecurityFirst

Powered by: MetaCompliance®
Making Compliance Easier™