SECURING INFORMATION IN THE MODERN WORKPLACE WITH HPE AND MICROSOFT

Bedrich Chaloupka
Global Collaboration Platforms Architect, Digital Workplace
Information protection is a set of techniques and best practices helping maintain information confidentiality, integrity and availability.

“Cyber security”
... deals with protecting data and information from outside sources in cyberspace or the Internet.

“Information security”
... protects information from unauthorized use, assess, modification or removal.
“Independently from whether the media keeping the information is physical or digital.”

INTRODUCTION TO INFORMATION PROTECTION
WHY DO I NEED INFORMATION PROTECTION?

Confidentiality
Information can be only accessed by those with the appropriate rights to view or manipulate it.

Integrity
Data and the information provided by them can be treated as reliable and accurate.

Availability
Data and the information provided by them can be accessed when and where needed.

Benefits of Information Protection

Compliance
Helps meet legal compliance and regulatory requirements

Usage rights
Understanding of information sensitivity helps better control access

User awareness
Better awareness of the information value the users are dealing with

User empowerment
Higher emphasis on information protection helps avoiding data leaks

Higher efficiency
Classification and labeling supports better findability and maintenance

Cost saving
Optimize storage consumption and investment into InfoSec toolset
## COMMONLY USED TECHNIQUES IN INFORMATION PROTECTION

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>Searching for a <strong>keyword</strong> or <strong>pattern</strong> that represents specific information, <strong>context</strong> to the information or an <strong>attribute</strong> common to a group if information.</td>
</tr>
<tr>
<td>Classification</td>
<td><strong>Process of categorizing</strong> data (representing the information) into groups to enable or improve information <strong>governance</strong> and <strong>protection</strong>.</td>
</tr>
<tr>
<td>Labeling</td>
<td><strong>Assigning</strong> to each group of information a <strong>visual sign</strong>, <strong>word</strong> or <strong>short phrase</strong> describing the key attribute of the information in the group.</td>
</tr>
<tr>
<td>Encryption</td>
<td><strong>Process of encoding</strong> an information in such a way that only <strong>authorized</strong> parties can <strong>access</strong> it.</td>
</tr>
<tr>
<td>Rights management</td>
<td>Applying certain <strong>access permissions</strong> that permit or deny an information recipient from <strong>taking</strong> certain <strong>actions</strong>.</td>
</tr>
</tbody>
</table>
KEY BEST PRACTICES

What you should think of before implementing Information Protection
THE MYTHS AND CHALLENGES OF INFORMATION PROTECTION

Long implementation cycle
Continuously growing amount of data in variety of repositories

Too complex to adopt
Limited knowledge of the data types and information sensitivity

Extra bureaucracy for users
It is seen by organizations as an extra task for information workers
#1: START WITH NEW AND ACTIVE DATA CLASSIFICATION AND PROTECTION

Information protection best practices
#2: THERE ARE ONLY TWO TYPES OF DATA – THE DATA THAT HAVE VALUE AND EVERYTHING ELSE

Information protection best practices
#3: The data with value are sensitive and can be easily identified with equation “PCI + PHI + PII + IP = SENSITIVE DATA”

Information protection best practices
#4: THE EXECUTIVE SUPPORT FOR THE CLASSIFICATION AND PROTECTION INITIATIVE IS MUST

Information protection best practices
#5: IT’S NOT ONE-MAN SHOW JOB – CLEARLY DEFINE ROLES AND RESPONSIBILITIES

Information protection best practices
MICROSOFT INFORMATION PROTECTION ECOSYSTEM

How do you assemble your box of bricks?

Office 365 Data Lost Prevention

Azure Information Protection Scanner

Windows Information Protection

Microsoft Cloud App Security

Sensitivity Labels

Azure Information Protection
automatic + manual using Office apps

Azure Rights Management
(used by OME, IRM, AIP)

Active Directory Rights Management Services
HPE SECURITY & INFORMATION MANAGEMENT SERVICES
Advisory & Professional Services – Digital Workplace

HPE Security Assessment Service for Microsoft 365
Periodic service providing your organization with insight into the recent changes in the Microsoft 365 security controls ecosystem, utilization of the security controls by the organization, development and review of the actionable plan implementation to improve the organization security posture.

HPE Information Lifecycle Management Services
This set of services provide your organization with assessment of the current information types and structures, Information Architecture, information access model and governance model design. Its helps your organization to support the compliance with industry regulations and improve utilizations of the information management tools for the benefit of the organization business.

HPE Security Standards and Compliance Assessment Service
HPE Security Standards and Compliance Assessment Service assesses an organization’s ability to protect their digital assets according to an internationally accepted code of security practices.

HPE Security Analysis and Roadmap Service
HPE Security Analysis and Roadmap Service analyzes the current state of security and controls in the context of your digital transformation target. It succeeds by identifying gaps and building a roadmap with actionable steps to strengthen security.
THANK YOU

Bedrich Chaloupka
bedrich.chaloupka@hpe.com
@BChaloupka_HPE