DLP Recommendations

The Dynamic Loss Prevention™ Report helps brokers and policyholders learn about IT exposures. The goal is to both improve understanding of the Smart Cyber Insurance policy itself, and to enable the policyholder to proactively mitigate their cyber risk. A critical part of this understanding is having actionable information, which is what the Recommendations portion of the DLP Report provides.

First, we want to be clear that the findings of the DLP Report are never used in a punitive fashion. Our mission is to give brokers who work with Corvus valuable information to share with their clients on a consultative basis, in a way that helps them prevent losses. The DLP report may flag a number of issues of both high and low impact, but these recommendations are only suggested actions. We will never negate or deny a claim because an insured did not take action on them.

WHO ARE THE RECOMMENDATIONS FOR?

These recommendations can help risk managers and other stakeholders in the insurance buying process to better understand their policy. Additionally, the recommendations are useful for anyone at, or affiliated with, your client's organization who manages their IT and web infrastructure. These recommendations are intended to help point IT managers to specific areas where they can impact overall cyber security for the company.

WHAT ARE THE RISK PRIORITY LEVELS?

We have tagged each of these risks as **High Impact**, **Medium Impact**, or **Low Impact** to help you better prioritize the overall risk. The recommendations are ranked according to their Impact tag, so you will see High Impact recommendations first. They are also categorized by the area of IT risk so that it is easy to understand how to address the issue.

DLP Recommendations

WHAT SHOULD I DO WITH THE RECOMMENDATIONS?

We provide you with a brief description of the issue and a recommended fix. In some instances, we'll recommend a software upgrade, but other times our recommendations may be more in alignment with an IT security policy change, such as implementing two-factor-authentication. In any case, the Recommendations are written so as to be easily understood by both technical and non-technical people.

THIRD PARTY RISK SERVICES:

Corvus policyholders are also provided with extensive third-party resources through our Risk Management Portal.

You can:

- Review the Breach Roadmap: your guide to how Corvus will respond in the event of a privacy breach. This detailed checklist helps you understand each point of the 11-step response process.
- Initiate a free consultation with an expert Breach Coach from Mullen Coughlin, one of the premier law firms dedicated to cybersecurity and data privacy. This consultation helps you determine what next steps are required for any potential breach.
- Access the Learning Center, a library of carefully selected information on a broad variety of hot-button cyber risk topics like cloud security, GDPR, social engineering and more. The Learning Center is continuously updated with new resources to keep your team up to date on the latest threats and trends.
- Use our suite of Risk Manager Tools - such as the Advanced Data Breach Cost Calculator, Common Vulnerabilities Assessment, and samples of information security and security training policies that could be implemented by your clients.
- Contact partner vendors from an approved list for pre-breach (defense) and post-breach (response), including security assessments, compliance readiness, IP protection, training, breach response and more. These select partners offer competitive rates for our policyholders.

The Risk Management Portal is available through our insurance platform, the CrowBar™. For more on how to access this resource see the Corvus Guide to Incident Response and Claims Handling.