cybersecuritylaw&practice

STRATEGIC ANALYSIS BY DATAGUIDANCE
VOLUME 01 ISSUE 06 SEPTEMBER 2015 WWW.E-COMLAW.COM

Cyber insurance market ripe for disruption

The cyber insurance market could grow to $7.5 billion in annual premiums by 2020 and the insurance industry could face competition from disruptors if it does not act fast to innovate, according to a new report 'Insurance 2020 & beyond: Reaping the dividends of cyber resilience' issued by PwC on 14 September.

"I'm not aware of any disruptors in this space currently. But given the proliferation of disruptors in financial services, we believe that it is only a matter of time before digital powerhouses, technology infrastructure and solutions companies, cloud service providers, professional services firms and cyber risk boutiques seek to collaborate to provide cyber risk protection and mitigation services, as well as post event remediation support, that may not be backed by a more traditional insurance offering that indemnifies financial losses and other liabilities," said Paul Delbridge, Partner at PwC.

The report includes suggestions on the types of innovations insurers could offer and suggests that insurers, reinsurers and brokers can capitalise on the cyber risk opportunity whilst managing the exposures.

IN THIS ISSUE

GCHQ advocates move away from complexity in passwords

The UK's Government Communications Headquarters ('GCHQ') published on 8 September 'Password Guidance: Simplifying Your Approach,' which provides organisations with advice on password policies and represents a change of direction for the agency, recommending a simpler approach to passwords.

"There is a small crisis building around the complexity of security measures - people are being asked to remember more and more pieces of increasingly complex information, which simply results in people forgetting them or writing them down," said Andrew Rogoyski, VP Cyber Security Services at IT consulting firm CGI. "GCHQ's new guidance is a welcome step to reverse that trend."

In explaining the need for a simplified approach, GCHQ says that users have an abundance of passwords, and complex passwords don't necessarily add to security but do create cost and cause delays. The guidance advocates measures including allowing users to securely record passwords, and only requiring users to change passwords when there is suspicion or indication of compromise.

"Forced password changes destroy entropy over time," said Paul Moore, an Information Security Consultant. "They promote password re-use and substantially weaken passwords across a larger area of the web - password becomes password1, for example. Although passwords may appear to have a finite value, the metadata they contain can often compromise future passwords. Such metadata includes character choice, style, complexity and crucially, password patterns gleaned from comparing user passwords over time."

Other recommendations include banning the use of password 'strength' meters, and instead implementing a list of predictable passwords that should not be used. But while the security community welcomes GCHQ's guidance, there's also a sense that the password as a concept has become outmoded. "Passwords have outlived their usefulness in their original form and must now evolve to recognise that humans are in the loop," argues Prof. Alan Woodward, Visiting Professor at the University of Surrey. "We also need to think about whether everything needs to be protected to the same degree - perhaps not everything needs a strong password and two factor authentication. If you needlessly pile on security you will simply compound the problem and users will suffer security fatigue."

Court rules that the FTC does have authority on data security

The Federal Trade Commission announced, on 24 August, that the US Court of Appeals for the Third Circuit issued their decision in *FTC v. Wyndham Worldwide Corporation*. The Decision affirms the ruling of the US District Court for the District of New Jersey, which held that the FTC did have authority to bring claims for lax data security practices under Section 5 of the FTC Act. The Decision also affirms that the FTC's informal guidance on data security can provide companies with fair notice of security practices which the FTC considers reasonable.

Kurt Wimmer, US Chair of Covington & Burling LLP's Privacy and Data Security Practice, commented, "Many companies are already taking cues from the FTC's informal guidance and its positions in consent orders, so for those companies the Decision will not change matters. For other companies that have been waiting for an answer to the question of what 'reasonable' security practices are, they will now need to assess their practices."

Commenting on the likelihood of a further appeal by Wyndham, Wimmer noted, "This decision doesn't settle the matter with any finality. Wyndham clearly will take one of two paths. It will either ask all the judges of the Third Circuit to rehear the case 'en banc,' meaning that all the judges would review the opinion of the three judges on the panel that decided the case. Or Wyndham will petition the US Supreme Court to review the Decision."