VORYS

Next Ten Tips for Data Breach Prevention and Response

Below are ten MORE tips that businesses of all sizes should consider in protecting the security and privacy of the data in their possession:

Use clear and consistent language in your data security policies: Conflicting and vague policy language creates uncertainty as to cybersecurity requirements and breach response measures.
Regularly download and install software updates: Periodic renewal of patches, firewalls and anti-virus maintains the robustness of system security and supports defenses that focus on reasonable efforts to protect data.
Segregate your system's databases and networks: Compartmentalizing the databases and networks on your system ensures that a breach of one part of your system does not become a breach of the entire system.
14 Encrypt sensitive data: Encryption of your company's sensitive data and your client/customer information protects against unauthorized access and use.
Regularly change passwords: Requiring your employees to regularly change their passwords keeps access credentials from becoming stale and creates "moving targets" that are more difficult for hackers to hit.
Insulate sensitive data and network locations from public access points: Have measures in place to ensure that guest Wi-Fi and public terminals cannot serve as backdoors into your company's network.
Suspend inactive accounts after termination or lack of use: Periodic removal of unused accounts eliminates a potential blind spot in your system's security.
Establish procedures for the preservation of data when a breach occurs: Resist the urge to format servers following a malware infection, so as to preserve important data regarding the extent of infection and possible exfiltration of data.
Require vendors to indemnify against breaches and other cyberliability: Include provisions in your company's vendor agreements that provide for indemnification if the vendor is the source of a breach of your data.
20 Carry appropriate cyberliability insurance: Insurers offer broad

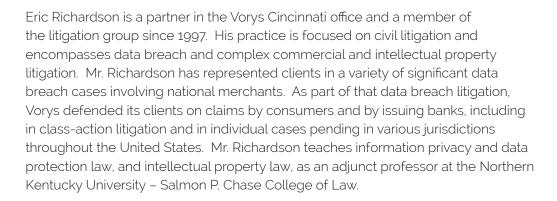
ranges of cyberliability insurance policies that cover many of the

cybersecurity risks that businesses of all sizes face.





Eric W. Richardson Mobile: 859.750.4069 Office: 513.723.4019 ewrichardson@vorys.com





Jacob D. MahleOffice: 513.723.8589
jdmahle@vorys.com

Jacob Mahle is a partner in the Vorys Cincinnati office. His practice is focused on government and regulatory investigations, defending False Claims Act matters involving CMS and the Department of Defense, representing retailers and financial institutions in data breach litigation, and counseling clients regarding privacy, data compliance issues, and incident response planning. Mr. Mahle teaches Information privacy law, and intellectual property law, as an adjunct professor at the Northern Kentucky University – Salmon P. Chase College of Law. He received his J.D. *summa cum laude* from the University of Cincinnati College of Law, where he was a member of the Order of the Coif, and his B.A. *summa cum laude* from Xavier University.



J.B. Lind Office: 513.842.8119 jblind@vorys.com

J.B. is a partner in the Vorys Cincinnati office and a member of the litigation group. Recognized for his work in complex commercial litigation matters, J.B. has particular experience with information privacy/data breach litigation, business litigation involving closely held or limited liability corporations, probate/estate litigation and intellectual property litigation. These specific focus areas led to J.B. being named an adjunct professor at the Northern Kentucky University – Salmon P. Chase College of Law teaching in the areas of information privacy and intellectual property. J.B. also handles cases in insurance and product liability/toxic tort litigation.



Brent D. Craft
Mobile: 606.922.3217
Office: 513.723.4072
bdcraft@vorys.com

Brent Craft is an attorney in the Vorys Cincinnati office and a member of the litigation group. His practice is focused on complex commercial litigation, *qui tam* and federal False Claims Act cases, government procurement, intellectual property law, and internal investigations. Brent also counsels clients on cybersecurity and data breach issues, including statutory notification requirements, regulatory compliance, and breach preparation and response. Brent received his J.D. *magna cum laude* from the University of Kentucky College of Law, where he was a member of the Order of the Coif and the *Kentucky Law Journal*. He received his B.A. from Transylvania University.