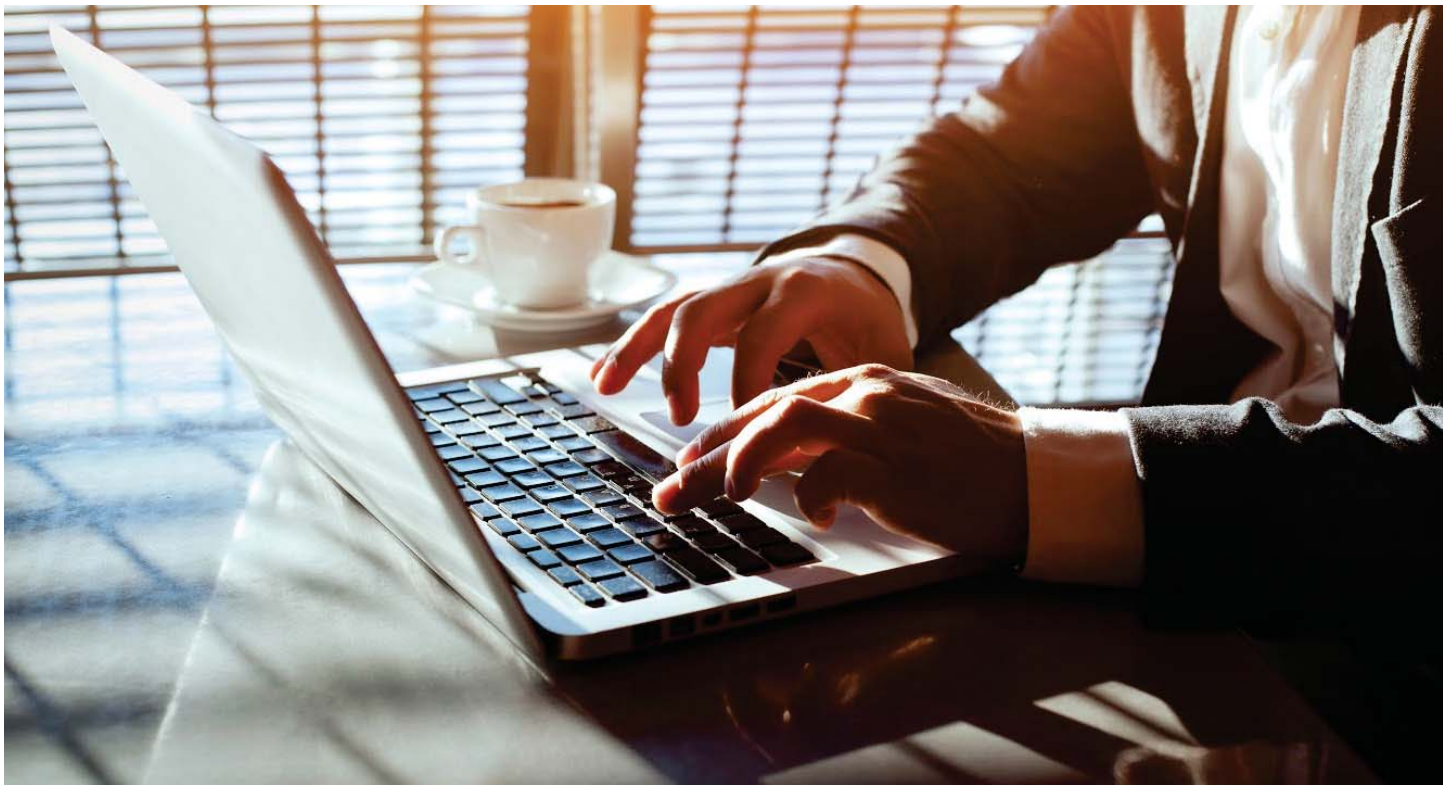
OPINION



Don't get robbed!

In the cyber age, with miscreants increasingly shrewd, insuring your firm against theft of monies and information is the order of the day.

Dan Knise

GUEST SPEAKER

Today more than ever, design firm leaders must be attuned to the growing risk of theft and disruption from hackers and other perpetrators. No longer can your focus be only on those who want to steal money from the petty cash drawer. In the current environment, you must keep an eye on your online banking and even your information; today's thieves have found value in data, in addition to money.

The use of the internet and online business and banking services is rapidly changing the nature of these risks and requiring increased emphasis on network security and sound risk management practices. It also calls for a review of your existing insurance policies to ensure you are adequately protected.

Consider some recent examples:

- **Fraudulent transfer of funds.** In checking its online bank statement, an engineering firm found an unauthorized $86,000 withdrawal. It discovered that someone, using malware, had been "shadowing" their computer key strokes and misappropriated their bank PIN and account information. With this information, the withdrawal was made without anyone's knowledge or consent. Crime insurance (also known as "employee dishonesty" or a "fidelity bond"), might have covered this claim; however, in this case the bank was on the hook for failing to follow its own authentication protocol.
- **Cyber extortion.** At another design firm, a client's electronic file folder "disappeared" from their system just days before construction drawings were to be delivered. In the ensuing panic, they also discovered issues with their back-up system and could not

"The use of the internet and online business and banking services is rapidly changing the nature of these risks and requiring increased emphasis on network security and sound risk management practices."

See DAN KNISE, page 8

DAN KNISE, from page 5

easily recreate the files. Thus, they were forced to pay ransom of $1,000 in bitcoin to the cyber criminals. Fortunately, the files were returned just in time for delivery to the client, but not without both a financial and psychological cost. In this case, the design firm had not yet purchased cyber/network security insurance. However, had they secured such a policy, they would have been covered under the "cyber extortion" section.

PROTECTING YOUR DATA AND YOUR MONEY. The first step in protecting your firm is to have a solid risk management plan, including:

- A system of financial controls that separates requests for payment from approvals, check issuance, and signature;
- Monthly reconciliation of bank statements and accounting records to track receipts and payables;
- Second approvals for any wire transfers or ACH transfers;
- A secure computer network that includes firewalls, encryption, anti-malware protection, and other barriers to unwanted intrusions;
- Back-up storage of data that allows you to quickly duplicate information that is lost, stolen, or compromised;
- Strong passwords (and don't forget mobile devices);
- Ongoing monitoring of computer systems including, potentially, intrusion testing; and
- Continual updating of systems, including installation of "patches."

"In the current environment, you must keep an eye on your online banking and even your information; today's thieves have found value in data, in addition to money."

INSURANCE CAN PROVIDE IMPORTANT FINANCIAL PROTECTION. Once solid risk-management measures are in place, the second block of a strong plan is to have appropriate insurances in case there is a loss. To address these risks, there are two key insurances that most design firms of any size should purchase:

- Crime insurance (also known as employee dishonesty or fidelity bond); and
- Cyber/network security insurance.

Both are relatively inexpensive and widely available in the insurance marketplace. A few key things to look for in each include:

CYBER/NETWORK SECURITY INSURANCE. Although several other insurance policies typically carried by design firms may provide some limited cyber/network security coverage (e.g., a sublimit on the package or professional liability policy), these "add-on" coverages often leave significant gaps. The only true protection is a stand-alone cyber/network security policy that covers both first-party costs (e.g., cost of notification and credit monitoring for affected individuals and business income lost due to a covered data breach or denial of service attack), and third-party claims (e.g., lawsuits alleging damages from a breach or costs incurred by your client for breach-related claims). Some key points about cyber/network security insurance policies are:

- **Typical limits carried.** $1 million to $5 million (note that various sublimits apply).
- **Coverage sections.** Typical coverage sections include: privacy and security liability, breach notification and regulatory compliance costs (also referred to as "event management"), public relations and forensic assistance expenses, business income interruption, cyber extortion payments and regulatory fines and penalties. Often, media liability is also included to protect against claims of copyright infringement.
- **Deductibles.** Deductibles usually range from $5,000 to $50,000, depending on size of the firm and limits purchased.
- **Other concerns.** Pay attention to issues such as: the definition of "confidential information," any prior acts dates/exclusions, whether or not there is a professional services exclusion (must be deleted or carved back), whether or not coverage is primary over any other available insurance.

CRIME/EMPLOYEE DISHONESTY INSURANCE. This coverage is often an add-on to a design firm's so-called package insurance policy which also provides general liability and property insurance. Generally, the limits of coverage provided under this approach are in the $25,000 to $100,000 range with a relatively narrow coverage grant. This is probably fine for smaller firms; however, firms with $5 million or more in billings should consider purchasing a stand-alone crime insurance policy. These policies often can be written for a three-year term and premiums are quite reasonable. Some key coverage issues to watch for include:

- **Typical limits carried.** Limits usually run from $500,000 to $5 million or more depending on the size of the firm's revenues and assets.
- **Deductibles.** Typically, $5,000 to $25,000, depending on firm size and limit purchased (higher limits tend to have higher deductibles).
- **Key extensions.** It is critical that the policy include funds transfer fraud and computer fraud. More claims are arising from these forms of theft (which, by the way, may be excluded from the coverage provided under your package policy noted above). Another key extension, "third party coverage," addresses loss of monies by a client or others if their funds are, for some reason, in your control.

PROTECTING YOUR FIRM. Solid risk management remains the most important way to protect your firm from cyber theft of data or monies. First, recognize the risk and develop a plan to protect your important assets – information and money. Next, train employees and ensure ongoing compliance. Insurance is, in many ways, the "belt and suspenders" protection to all your other actions. And cyber and crime insurers have a wealth of resources to assist you in preventing loss; some purchase the insurance primarily to gain access to these resources.

In this challenging risk environment, continued vigilance is definitely the order of the day!

DAN KNISE is the president and CEO at **Ames & Gough**. Contact him at dknise@amesgough.com.