Processes should be put in place to limit breach damage, bolster defenses and help repair the brand, reports Larry Jaffee.

With apologies to English songwriters Anthony Newley and Leslie Bricusse, it’s a new dawn, a new breach…

Considering the current climate, are organizations changing the way they do business, assessing their vulnerabilities, taking stock of and protecting the crown jewels, and getting prepared for the time when/if the network does get breached, damage will be minimized and operations will not be crippled indefinitely?

Well, at least some appear to be doing so. The onslaught of cyberattacks have caught the attention of the C-suite in all sectors alerting them to the importance of warding off potential threats.
Continuity planning

Staffing and investment levels for state-of-the-art IT security planning are slowly rising, and not too soon, concur IT security experts.

“It’s a pattern that we’re brought in almost always after there’s a problem, rather than before,” says Larry Ponemon, chairman and founder of the Ponemon Institute, a Traverse City, Mich.-based research think tank dedicated to advancing privacy and data protection practices. “The problem at least gets them to think more seriously about the issue. Board members start to worry that [the event] will damage their legacy or they might have personal liability.”

A sea change is occurring, altering perspectives on who is accountable with aawning recognition that risk falls on the board and the business, not just the security team and the CISO, agrees Raj Samani, London-based vice president and CTO at McAfee EMIA, part of Intel Security.

Samani points out that a board will recognize the future ROI benefit in beefing up security when alerted to the potential of a three to five percent sales decline following a data breach.

Further, marketing, PR, legal and all other departments need to be involved in breach response to ensure business continuity, which should be laid out in an existing crisis plan that anticipates unwanted eventualities.

“The awareness level has gone way up,” says Tom Smith, VP of business development and strategy at Gemalto. A 2015 report on cybersecurity from the global digital security company, found 89 percent of IT pros surveyed reported “some impact from recent security breaches,” of which approximately half raised concerns, while 40 percent were actually re-evaluating or changing policies.

As a best practice, predictive models should be deployed, says Gene Fredriksson, CISO for PSCU, a Saint Petersburg, Fla.-based provider of PCI transaction clearance for more than 800 credit unions. “Rather than running around with your pants on fire playing Whack-A-Mole, [you] at least have an idea on what your priorities should be. Too often organizations just focus on warding off inbound attacks, Fredriksson says, “getting only half the picture.” Potential inside threats within your infrastructure must be vigilantly monitored. For example, an unauthorized connection from a computer to a command-and-control server in China is a pretty huge red flag that the machine needs to be shut down. “Once you understand where the bad guys are coming from, you can start to be proactive,” he says.

Know what’s on your network

Monitoring a company’s computers is not about “Why is Wayne spending so much time on Facebook? It’s why Wayne’s computer always transferring all this data over DNS and returning all these DNS query responses in the middle of the night?,” points out Chris Coleman, CEO of Lookingglass, an Arlington, Va.-based cyber threat intelligence management firm.

Inside breaches typically involve an employee copying data from an office workstation, agrees James Knight, owner of New York-based company Beta Unlimited, which provides Mac-based forensics. “External hacks wouldn’t login into a file server to copy files, but gets at the files through some sort of security hole.” For clients looking to protect sensitive data, Knight writes “a script to alert when multiple files are opened from one IP address in quick succession, which usually indicates a copy is happening.”

Poor asset management is usually at the core of most IT security incidences, points out Ron Gula, CEO and CTO of Tenable Network Security, a Columbia, Md.-based provider of continuous network monitoring to identify vulnerabilities.

“If you don’t have knowledge of what’s on your network, how can you possibly manage it? You won’t be able to detect intruders,” Gula warns.

A byproduct of the recent deluge of breaches is that some organizations are “unfortunately doubling down on maybe ineffective practices– just buying security defensive products,” Gula says. They’re stuck in a “vulnerability treadmill,” doing some sort of periodic security audit, getting a big report of vulnerabilities. Those companies work hard to get rid of them, never improving, constantly see-saving up and down. Such companies typically do not patch effectively on a continual basis.

Just because an organization is regulatory compliant doesn’t necessarily mean the enterprise is secure. Just ask Anthem and Premara Blue Cross.

Larry Ponemon, chairman and founder of the Ponemon Institute, believes that even though Anthem had a strong security posture, it still couldn’t stop a recent breach.

“No one would have expected that the records could have been exposed,” he says. “Even though Anthem had a strong security posture, it still couldn’t stop a recent breach.”

Arlington, Va.-based cyber threat intelligence management firm, believes that the bad guys are coming from, you can start to be proactive,” he says.

Pointing out the whereabouts and number of copies of all data is critical, Gula says. “Cloud providers aren’t necessarily a weak link. “If you’re going to put your data in somebody else’s house, then protect their house [with encryption],” Cates advises. “Quite often the service provider is better at security than you. But you want to keep the key just in case they’re comprised.”

Another preventive measure is removing potential risk from administrators. Hackers can’t steal what you possibly manage it? You won’t be able to detect intruders,” Gula warns.

A byproduct of the recent deluge of breaches is that some organizations are “unfortunately doubling down on maybe ineffective practices– just buying security defensive products,” Gula says. They’re stuck in a “vulnerability treadmill,” doing some sort of periodic security audit, getting a big report of vulnerabilities. Those companies work hard to get rid of them, never improving, constantly see-saving up and down. Such companies typically do not patch effectively on a continual basis.

Bad reputation

Aside from technical actions, Cates advises that – before a breach – organizations proactively align themselves with experienced outside counsel that has previously waded through the legal aspects of a breach. “They already have the expertise from other clients. Counsel can be an enabler in getting your response team together.”

It is very hard for organizations following a breach to recover reputation-wise. The brand almost always suffers damage from not only a customer perspective, but also business partners. “Reputational cost is difficult to measure, and because it isn’t measurable insurance won’t cover it,” notes Ponemon, admitting that what’s missing from his firm’s company’s cost analysis model is long-term reputational effect.”

He believes a landmark judicial award involving a class-action suit resulting from a data breach is likely to occur soon that will determine an organization’s exposure.