How to Improve Cyber Security with Enterprise Architecture

Marc Lankhorst

Introduction

It is no secret that cybersecurity threats are ever increasing. It is sometimes said there are only two kinds of organizations: those who know they have been breached, and those who do not know it yet. To mitigate the risk and damage associated with cybersecurity, it is important to know how to assess these risks and improve your defenses via security-by-design. It is also important to plan for what to do if (and when) things do go sideways. So, let us have a look at some important steps that you can take to effectively manage risk and stay as safe as possible in this dangerous world.

5 Steps to Boost Your Cyber Security

Ensure enterprise-wide awareness

In most organizations, upper-level management awareness of cyber threats has increased due to the many high-profile incidents over the last few years. The cost associated with ransomware, data breaches and other issues can easily reach in the hundreds of millions. But too often, many still see cybersecurity as a technical issue, to be dealt with by the IT director and his or her underlings. One sure way to wake up the boardroom to cybersecurity awareness is regulatory compliance. In these instances, management can be held personally responsible for non-compliance, so there is a strong incentive to act.

New regulation on data privacy, such as the EU's GDPR, is only one example where security and privacy concerns have reached the boardroom. Sector-specific and regional regulations, such as the US HIPAA Privacy Rule for the healthcare sector or the NYDFS Cybersecurity Regulation for the financial services sector in New York, are other examples. But often, management feel like deer in the headlights when it comes to cyber threats. They see the danger but do not know what to do in the face of these threats. The breadth and depth of these issues may indeed seem incomprehensible and unsolvable. To help management overcome such paralysis, you must present solutions, not just problems. Enterprise architects are uniquely positioned to provide these. We will address the issue of talking to stakeholders on security in more detail a bit further down the line.

Align security and risk management with business strategy

To spend your money wisely, you will need to invest in security where it really counts – that is, where it is strategically important. You should, therefore, classify your assets according to their strategic importance, considering regulatory compliance and other guidelines. What are these assets worth, not just in financial terms but in a broader sense?

For example, protecting valuable intellectual property or privacy-sensitive data may be crucial for your business continuity or essential from a regulatory compliance perspective. Such a classification helps you decide on investment priorities and avoid spending too much on protecting unimportant assets or blanket measures.

Unfortunately, many organizations do not have a clear connection between their strategy and assets. A solid enterprise architecture related to strategic direction and motivation, as well as to implementation within in the organization, offers the "connective tissue" you need. Enterprise Studio offers the integrated support for describing strategy, architecture, processes, systems, and data, which is key to creating such a line of sight.

Analyze your vulnerabilities and risks

Cyberattacks are becoming increasingly sophisticated, using a combination of digital, physical, and social engineering techniques. A common example is the so-called "road apple attack." A would-be intruder "accidentally" leaves a USB flash drive in a public spot such as the company car park. An employee picks it up, and chances are that he will not be able to suppress his curiosity and plug it into his PC. Surprise: the drive is infected with malware that infects the PC and sends sensitive information to the intruder.

You must take an integral approach to defend against such attacks, incorporating all aspects of your enterprise, including personnel education, processes, and procedures, as well as technical measures like firewalls and antivirus software. Moreover, you should look at this from the perspective of your business goals and strategy, as mentioned before.

With Enterprise Studio, you can capture and visualize various risk and security aspects of your organization. It helps you get a better grasp of hazards, risks, and mitigation measures in relation to your overall architecture, business strategy and assets so you can perform a true strategy- and value-based risk and compliance assessment. You can measure and visualize the potential impact of these risks and use these insights to prioritize investments in mitigating measures as part of the next step.

Take a security-by-design approach

Vulnerabilities should not be fixed after the fact, especially not by just slapping on some ad-hoc security measures like an extra firewall. Rather than defining a separate security architecture, you should develop a secure architecture and address risks proactively in the architecture and design across all levels of your enterprise, from people and responsibilities to processes and technology.

You also need to consider your organization's position in the broader ecosystem. Having your own house in order may not be enough. For instance, if you rely extensively on some external partner, their security may be business-critical for your own operations. Some organizations try to rely on contracts and agreements to take care of this, but that may be insufficient.

Legally, you may be held responsible for a breach at, say, an outsourcing partner. Regulation such as the GDPR explicitly states that your organization remains liable for the processing of privacy-sensitive data, even if you hire someone else to do that for you. In some cases, you may even need to have your business partners audited to remain compliant.

In a security-by-design approach, you prioritize investments in security based on the value of your assets and the vulnerabilities you have found in the previous steps. You calculate the business value and impact of security projects and use this to make a prioritization of IT measures. Our platform can help you clearly identify where to spend your budget most effectively, thanks to its enterprise portfolio management capabilities.

Assume you are compromised

No amount of security measures will make you 100% safe, so you had better be prepared to act when things go sideways. Many organizations scramble to find out what to do when they are compromised because they don't know which parts of the organization or its systems might be affected.

Creating contingency plans based on clear insights into the structure and operations of your enterprise is essential. Up-to-date models of your architecture, processes, systems, and data can be a tremendous help in assessing how far a problem could spread, and at which points you should act quickly to limit the impact of a security breach.

But remember Eisenhower's dictum: "Plans are nothing; planning is everything". Nothing ever goes completely according to plan, but the development itself of such plans will make clear what you need to know, what the unknowns are and where you need to update your knowledge of your enterprise's make-up. Connecting Enterprise Studio with systems such as CMDBs, which administer and monitor operational reality, helps to ensure that you use the best and most timely data available.

Finally, all this information needs to be readily accessible for your organization's "first responders". BiZZdesign's platform's publishing capabilities offer a great solution, with easy-to-use views and dashboards for different types of users, ranging from business decision makers to operational management, and people on the proverbial shop floor.

Analyze Your Security with Architecture Models

So far, we talked about the essential steps to keep your organization safe in an increasingly dangerous digital environment. As we move forward, I want to zoom in on which instruments to use to help you achieve cybersecurity — in particular for steps 3 and 4. It will not surprise you that we advocate a model-based approach to analyzing and mitigating cyber risks. Clear, formalized descriptions of your enterprise will help you gain the understanding necessary to provide optimal security solutions.

Of course, you cannot achieve absolute security. Rather, you should focus on where you need to invest from the perspective of 1) the value of the assets you want to protect and 2) the vulnerabilities associated with these assets. Our approach to enterprise risk and security management (ERSM) is based on several open standards, most notably the ArchiMate standard for enterprise architecture modeling, as well as the Open FAIR standard for information risk

management. More details are described in The Open Group's white paper on modeling enterprise risk management and security.

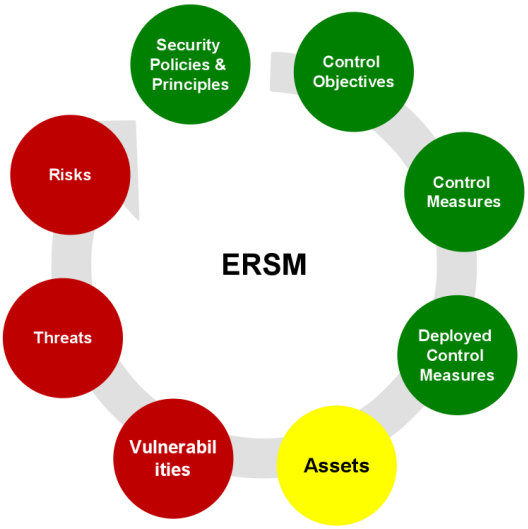

Figure 1: The steps to our approach to enterprise risk and security management

Figure 1 shows the main steps of our approach, which is built into Enterprise Studio's Governance, Risk & Compliance functionality. At the bottom of the image you see the assets you want to protect from cyber risks, while at the top we see the policies, principles and objectives that direct the organization.

In between are the steps that connect these. On the left side (in red), you see the analysis of cyber risk in your organization. On the right side (in green) you see the implementation of controls to improve your security. These are the steps of risk and security management:

1. *Review assets*

What are the most important assets that are critical to your enterprise? What do applicable regulations say about these assets? For example, the personal data of your customers may be one such asset. Your reputation as a trustworthy organization may be another. Can you put a value to these elements? That will help you later when deciding what is most important to protect.

2. *Analyze vulnerabilities*

In what ways are your enterprise's assets vulnerable? In cyber security, "zero-day vulnerabilities," which are not known to anyone but the attacker, are of course the most dangerous and will naturally not show up in this list. But you should investigate other vulnerabilities you can recognize and link these to the assets they expose. You can reuse the models of your business and IT architecture, augmenting them with relevant security aspects.

3. *Assess threats*

After you assess your asset-specific vulnerabilities, you need to assess whether these vulnerabilities could really be exploited by so-called "threat events" and "threat agents." These

can range from malicious hackers to hostile governments, as well as your own staff, technical malfunctions, natural disasters, and other accidents. We have collected an extensive model of hundreds of common vulnerabilities, threat agents and threat events, which can serve as a starting point for your analysis in this and the previous step.

4. Calculate risk

Based on potential threats and the value of your assets, you can assess the risks your enterprise faces. In a simple formula, risk = value x probability, the higher the risk, the more you will want to invest in mitigating against it. Figure 2 shows an example of such an analysis, gradually built up in these first four steps.

The lower part of the model shows the infrastructure and the asset you want to protect ('Encrypted payment record'). The upper part shows:

- Two vulnerabilities ('Insecure transmission channel' and 'Weak encryption of payment data')
- The threat agent ('Cyber criminal')
- A threat event ('Man-in-the-middle attack')
- A potential loss event resulting from this threat ('Unauthorized payments')
- The resulting risk ('Financial loss')

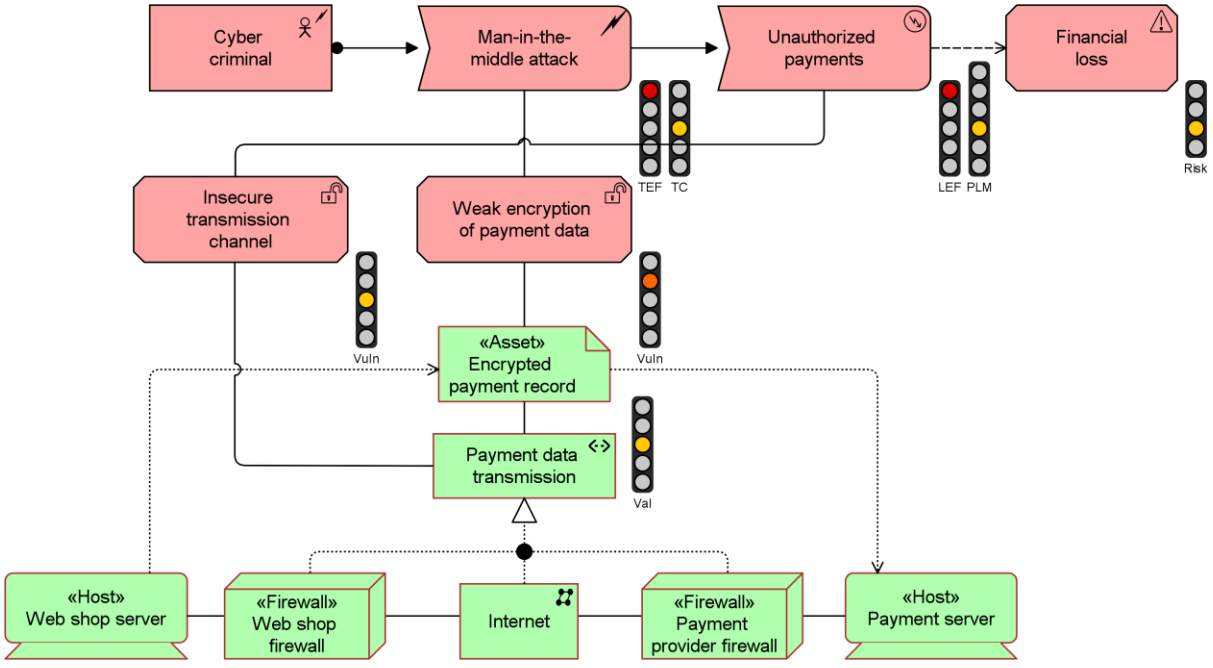

Figure 2: Risk analysis example

The traffic lights show various parameters, such as the asset value, vulnerability level and the resulting risk level. All these are connected, and our risk analysis algorithm calculates the results, e.g. increasing the risk level if you increase the asset value or threat capability.

5. *Create policies*

To deal proactively with potential cyber risks, you should define appropriate security policies and principles that are in line with your business strategy and follow applicable regulations. This may, for example, include principles such as security-by-design, separation of duties, restricted access to personal data and other common policies. Regulatory frameworks like the GDPR demand solid data protection policies, with hefty fines for non-compliance and even personal liability of responsible management. This, in turn, influences the value of the assets you want to protect. It is not just their intrinsic value at stake – fines, reputational damage and other side effects should also be taken into account.

6. *Define control objectives*

Based on the policies you created in the last step, you should now define the right control objectives. One standard approach is to classify the confidentiality, integrity, availability, privacy-sensitivity, and other attributes of your data, according to common use cases you have. For instance, data on your website will need low confidentiality but high availability, while customer data will have much higher privacy and confidentiality requirements, while availability might be less of a concern.

7. *Create control measures*

These control objectives are then translated into applicable control measures, which tell you what to do to achieve these objectives. Relevant standards, such as ISO/IEC 27001, NIST 800-53, CSA and others may help by providing a predefined and well-organized set of control measures. Below, in Figure 3, you see a small excerpt from a model of the ISO/IEC 27001 standard, showing one specific control objective and related control measures, expressed in the risk and security overlay of ArchiMate that is defined in the Open Group whitepaper mentioned previously. Figure 4 shows a set of controls from the CSA standard, applicable to encryption.

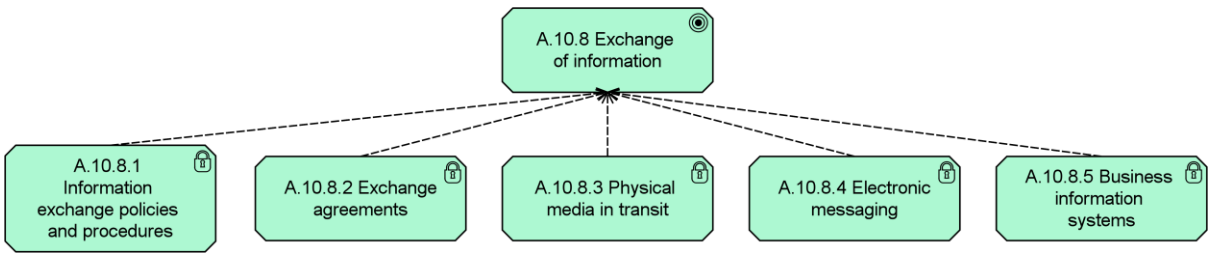

Figure 3: ISO/IEC 27001 example control objective and measures

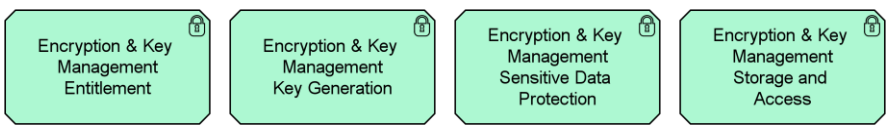

Figure 4: CSA Controls for Encryption and Key Management

8. *Implement control measures*

The last step is to design the implementation of these control measures as part of your own architecture, processes, and systems. For example, you will need to figure out how you implement encryption and key management (the measures from Figure 4). You can compare the cost of implementing these measures with the risks you run. Are they worth it, or are you protecting low-value assets with overly expensive controls?

The analysis shown above is, of course, done by modeling and risk assessment experts and may look complicated to the uninitiated. However, you can present the results in user-friendly heatmaps like the one in Figure 5. The heatmap in Figure 5 shows how high capability of threats (e.g. smart hackers) combined with low strength of controls results in a very high vulnerability level. The other two vulnerabilities in this heatmap are less urgent.

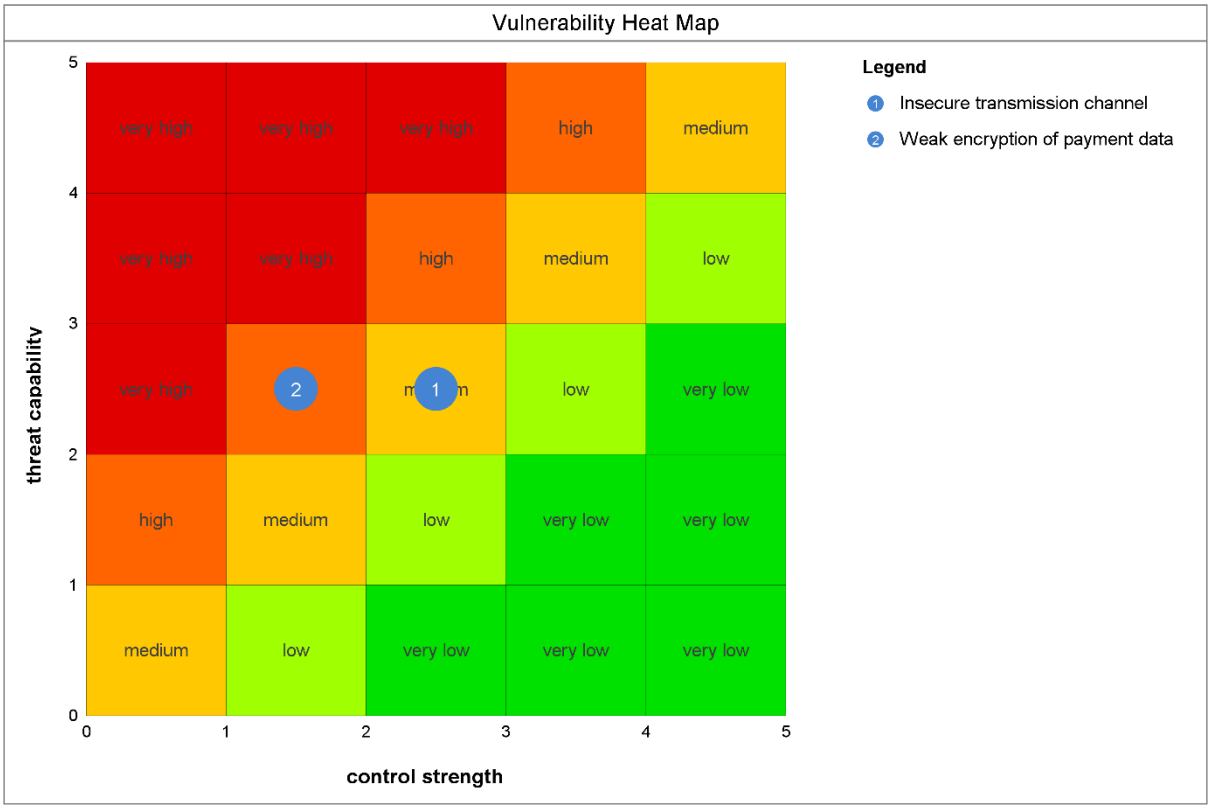

Figure 5: Risk analysis heatmap

This analysis helps management prioritize investments in improving security like, in this example, implementing rules on password length or instituting multi-factor authentication. Thus, your organization has room in its budget to invest where it really counts. Remember that security architecture is a continuous concern. Risk management, too, is a continuous, iterative process.

You should run the process outlined above on a regular basis to assess new vulnerabilities and threats and to keep your policies, principles and controls updated with your organization's strategy and applicable regulatory demands. In fact, various regulatory frameworks require you to have such a risk management process.

Embedding this within your regular architecture and design processes provides you with a security-by-design approach — a much more effective way to improve your organization's resilience than simply tacking on some security measures after a cybersecurity event. There is no guarantee that nothing will ever go wrong. Nevertheless, having such a model-based approach to risk analysis and mitigation will prove to be a great investment in your organization's cyber security, business continuity and resilience where (and when) it really counts.

How to Communicate about Cyber Security

As promised earlier, let us turn again to the subject of communicating about cyber security. We will go over some tips on how to involve your business more, what really works when it comes to building security awareness, as well as what practices to avoid.

To begin with, is it really necessary to communicate about risk and security architecture? And if so, to whom? And what? Well, communication is in fact integral to the process, and you should think of decision-makers as your target audience, since the business needs to be well-informed if it is to make the right decisions. As enterprise architects trying to build in cybersecurity processes and standards, you need to involve and inform not just management, but the rest of the organization as well.

What you communicate also matters and is more difficult to decide since the differences between business decision-makers are enormous. Personal interests, backgrounds, levels of education and professional sector are all important variables. Nonetheless, we would like to offer you a list of best practices that is sure to help you in defining a good approach.

1. Risk does not hurt. The impact does!

Typically, risk managers and security architects try to gain the attention of their managers and executives in two ways. One popular method is to target fear and pain. They communicate the potential impact of risks on the business. Alternatively, some professionals present the potential gain of being successful in security, e.g. more trust from customers. In general, selling fear beats selling the gain of being secure. This is known as "loss aversion": people prefer avoiding losses to acquiring equivalent gains.

2. Use metaphors

Metaphors are extremely effective in communicating more complex concepts to your business management. For example, you can simplify the discussion by comparing information security to insurance. Everybody has some form of insurance. Many people have more insurance than they really need. Of course, most people hope they will never need it but they buy it anyway, just in case.

Another good metaphor is that of traffic. Some managers like driving at a high speed. They know that things can go wrong and they could end up with some form of penalty, but often they are willing to accept this risk. Some managers might never drive more than 50km/h above the legal

limit because they know they might lose their license. Others might use apps to determine where the police has its checkpoints. When you use metaphors, risks become easier to understand than most abstract cybersecurity terminology. This helps to advocate the importance of risk management.

3. Show concrete examples

Only a small percentage of hacks (perhaps a few percent) are ever made public. Still, these can really help people internalize what the potential consequences of breaches are. Use these! And be smart about it, choose cases from your own industry and/or country to ensure it hits close to home.

4. Test security

Most professionals have to stand in front of their building every month when yet another fire drill takes place. Sure, it is inconvenient, but we all understand that it has a clear purpose. Real-life testing of computer issues is done with penetration tests, for instance. But the business itself and especially the management team are hardly ever affected by these tests.

Try to organize experiences involving real life testing of security leaks, attacks, and downtime tests. This does not only provide you with relevant information, but also helps to give your stakeholders a sense of urgency about the topic.

5. Use stakeholder-specific communication

"The business" is not one person. It is made up of a large audience ranging from on-the-floor employees, team leaders, non-tech, semi-tech, and technical stakeholders to board members and maybe even sourcing partners. These groups have different information needs and need different communication styles. Define communication strategies that present the right security information to the right people, through the right channel and in the right format. Just be careful not to offend management by presenting information that has been overly simplified.

6. Don't use jargon, and if you really have to, use business jargon

Architects understand the distinction between conceptual, logical, and physical models and consider the methods that need to be applied. But managers are indifferent to this. The only jargon they are fluent in, is the jargon of your business. Money, speed, and risk is the jargon to use in the boardroom. So, when you are pleading your case, be sure to relate measures to potential financial or image losses. This is likely to help them engage board members in the topic of information security.

7. Make it personal

The key message that should be ingrained in a business manager's mind after a meeting on information security awareness should be: "This is a serious issue". Or more concretely: "This affects me/my position/my people/my customers/my career". Discussing these topics only at large

meetings will not really help you to get feedback and learn if your message has landed. Do not talk *at* the managers you want to have on board your information security train, talk *with* them!

Here are some of the approaches that, in our experience, work quite well to build information security awareness:

- *What's in it for me?* Although the interests of an organization as a whole regarding information security are understood by most employees, personal interests still seem to be more urgent for many. Try to exploit this fact by telling people what they stand to lose, e.g. reputation, trust, business continuity, money, data, time, whatever is most relevant to them.
- *What if this was your company?* Asking someone what they would do if it were their company facing information security problems is a great way to get honest responses. This is a personal question, which gets people to think of the bigger challenge, not just their own little tasks.
- *Security hero of the month*: Rewarding good behavior is a simple yet effective mechanism. Praising those that perform well with some simple rewards, and compliments from management can make a major difference.
- *Drip vs. tsunami messaging*: It is bad practice to flood your audience with a huge information load once or twice a year. Instead, sharing short messages often (as opposed to long messages rarely) does a much better job of keeping security at the top of people's minds. Keep reminding them of your vision and repeat what you expect people to do.
- *Make it real*: A hacking demonstration can shine a light on this question. There is no need to show the technical part, just the part where you show what the damage is.

Creating awareness really is a challenge, but with the best practices mentioned above things might become a little easier. The BiZZdesign suite helps you leverage existing architecture and portfolio models and data in order to give you a flying start when it comes to improving your data security and ensuring regulatory compliance.

Our integrated approach helps you invest in security where it counts and avoid the penalties and reputational risk of non-compliance, or worse, of a data breach. If you'd like to learn more about how our platform can help you enhance your cyber security, please get in touch today or request a free live demo!

About BiZZdesign

BiZZdesign is a leading enterprise transformation software vendor based in the Netherlands. Founded in 2000 as the commercial spin-off of an R&D institute, today the company enjoys a global presence and is recognized by industry analysts as a market leader. BiZZdesign's flagship product, Enterprise Studio, is deployed in blue chip companies and government organizations across all continents, where it plays a key role in enabling meaningful business change.

For more information, please visit www.BiZZdesign.com.